Support contract on financial scams Study

Final Report

Written by Spark Legal and Policy Consulting and Open Evidence

Internal identification

Contract number: 300144551

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content and Technology
Directorate D – Online Platforms: Economy
Unit D.3 – e-Commerce

Contact: CNECT-D3@ec.europa.eu

European Commission
B-1049 Brussels

SUPPORT CONTRACT ON FINANCIAL SCAMS STUDY

Final Report

Directorate-General for Communications Networks, Content and Technology

2026 EN

EUROPE DIRECT is a service to help you find answers to your questions about the European Union

Freephone number (*):
00 800 6 7 8 9 10 11

(*) The information given is free, as are most calls (though some operators, phone boxes or hotels may charge you)

LEGAL NOTICE

This report was commissioned by the European Commission, Directorate-General of Communications Networks, Content & Technology. The information and views set out in this report are those of the author(s) and do not necessarily reflect the official opinion of the Commission. The Commission does not guarantee the accuracy of the data included in this study. Neither the Commission nor any person acting on the Commission's behalf may be held responsible for the use which may be made of the information contained therein.

Manuscript completed in August 2026

The European Commission is not liable for any consequence stemming from the reuse of this publication.

Luxembourg: Publications Office of the European Union, 2026

© European Union, 2026

The reuse policy of European Commission documents is implemented by the Commission Decision 2011/833/EU of 12 December 2011 on the reuse of Commission documents (OJ L 330, 14.12.2011, p. 39). Except otherwise noted, the reuse of this document is authorised under a Creative Commons Attribution 4.0 International (CC-BY 4.0) licence (https://creativecommons.org/licenses/by/4.0/). This means that reuse is allowed provided appropriate credit is given and any changes are indicated.

For any use or reproduction of elements that are not owned by the European Union, permission may need to be sought directly from the respective rightholders.

PDF ISBN 978-92-68-44336-1 doi: 10.2759/7359032 KK-01-26-169-EN-N

Contents

Table of Abbreviations **9**

Glossary **12**

Abstract **17**

Executive Summary **18**

Synthèse **23**

1. Introduction **28**

1.1. Study objectives and scope 28

1.2. Methodological approach and report structure 29

2. Typological mapping of online financial scams **32**

2.1. Investment scams 37

Traditional investment scams 38
Cryptocurrency scams 40

2.2. Romance scams 45

Traditional romance scams 45
Romance baiting 49
Sextortion 50

2.3. E-commerce scams 52

Undelivered products or services 52
Counterfeit products 54
Health and wellness scams 56
Event ticket scams 57
Subscription scams and hidden renewals 58
Artificial streaming scams 59
Insurance scams 60
Loan and credit offer scams 61
Rental scams 63

2.4. Employment and collaboration scams 65

Fake job scams 65
Money mule recruitment 66
Direct Message (DM) to Collab bots 67

2.5. Unexpected gain scams 68

2.6. Charity and disaster relief scams 71
Charity scams 71
Fraudulent crowdfunding campaigns 72

3. Operationalisation of online financial scams on online platforms 74

3.1. Platform features as financial scam dissemination channels 75
3.1.1. Overview of risk factors identified by third parties 75
3.1.2. Overview of risk factors identified by designated service providers 92
3.2. Cross-platform considerations 99
3.2.1. Cross-platform pathways 99
3.2.2. Adaptable nature of scammers 105
3.2.3. Operational tools 106
3.2.4. AI as an amplifying element 112
3.2.5. Social engineering methods 114
3.2.6. Fraud-as-a-service infrastructure 117

4. Social and economic impact of online financial scams 120

4.1. Victims of online financial scams 121
4.1.1. General patterns of victimisation 122
4.1.2. Scam-specific patterns of victimisation 125
4.2. Economic impact of financial scams 133
4.2.1. Societal-level economic impact 133
4.2.2. Individual-level economic impact 134
4.2.3. Economic impact by type of scam 136
4.3. Social impact of financial scams 142
4.3.1. Societal-level social impacts 143
4.3.2. Individual-level social impacts 143
4.3.3. Social impact by type of scam 145

5. Countermeasures 149

5.1. Access and gatekeeping measures 149
Measure 1: Identity requirements for personal accounts 149
Measure 2: KYBC requirements 153
Measure 3: Ad placement requirements 157
Measure 4: Labelling AI-generated content 164
5.2. Detection and removal measures 168
Measure 1: Automated detection systems 168
Measure 2: Human review 174
Measure 3: Removal and suspension mechanisms 177
Measure 4: Detection of coordinated scam networks 184
Measure 5: Recommender system protection measures 187
5.3. User-facing protection measures 190
Measure 1: Reporting tools 190
Measure 2: Information on redress 197
Measure 3: Friction tools 201

5.4. Structural level governance and policies 205
Measure 1: Platform-level policies 205
Measure 2: Cooperation with third parties 208

6. Case studies 213

6.1. Case study A: Finfluencers and online coaching on video-sharing platforms 213

6.2. Case study B: Romance baiting scams on social media platforms 224

6.3. Case study C: Fake webshop advertisement on search engines 232

6.4. Case study D: Health and wellness scams on e-commerce platforms 245

7. Conclusions 259

8. Annexes 262

Annex I – List of sources 263

Annex II – Interview guide for Task 1 296

Annex III – Interview guide for Task 2 298

Annex IV - Workshop Report 299

1. Scam Typology 301
2. Risk Factors 303
3. Countermeasures 306
4. Case Studies 309

Annex V - Overview of measures as reported to have been implemented by designated service providers 312

Identity verification measures for account creation 312

KYBC requirements 315

Ad placement requirements 320

Labelling AI-generated content 325

Automated detection systems 329

Human review 334

Removal and suspension mechanisms 336
Detection of coordinated scam networks 339
Recommender system protection measures 342
Reporting tools 345
Information on redress 356
Friction tools 359
Platform policies 362
Cooperation with third parties 366

Table of Abbreviations

Abbreviation	Full Term
ABBL	Association of Banks and Bankers, Luxembourg
ABI	Association of British Insurers
ACAMS	Association of Certified Anti-Money Laundering Specialists
ACM	Autoriteit Consument en Markt (Netherlands Authority for Consumers and Markets)
ACPR	Autorité de contrôle prudentiel et de résolution (French Prudential Supervision and Resolution Authority)
AFM	Autoriteit Financiële Markten (Netherlands Authority for the Financial Markets)
AI	Artificial Intelligence
AIT	Austrian Institute of Technology
AMF	Autorité des Marchés Financiers (French Financial Markets Authority)
AML	Anti-Money Laundering
API	Application Programming Interface
BaFin	Bundesanstalt für Finanzdienstleistungsaufsicht (German Federal Financial Supervisory Authority)
BEUC	Bureau Européen des Unions de Consommateurs (The European Consumer Organisation)
CC BY 4.0	Creative Commons Attribution 4.0 International
CCPC	Irish Competition and Consumer Protection Commission
CDD	Customer Due Diligence
CMA	United Kingdom Competition and Markets Authority
CPC	Consumer Protection Cooperation (Network)
DG CONNECT	Directorate-General for Communications Networks, Content and Technology
DGCCRF	Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes (French Directorate-General for Competition, Consumer Affairs and Fraud Prevention)
DM	Direct Message
DSA	Digital Services Act (Regulation (EU) 2022/2065)
DSC	Digital Services Coordinator
EBA	European Banking Authority
EC3	European Cybercrime Centre (Europol)
ECB	European Central Bank
ECC-Net	European Consumer Centres Network
EDMO	European Digital Media Observatory
EIOPA	European Insurance and Occupational Pensions Authority

Abbreviation	Full Term
EMA	European Medicines Agency
EMPACT	European Multidisciplinary Platform Against Criminal Threats
ENISA	European Union Agency for Cybersecurity
EPUB	Electronic Publication
ESMA	European Securities and Markets Authority
EU	European Union
EU FRA	European Union Agency for Fundamental Rights
EUIPO	European Union Intellectual Property Office
EUR	Euro
FaaS	Fraud-as-a-Service
FATF	Financial Action Task Force
FBI	Federal Bureau of Investigation
FCA	Financial Conduct Authority (United Kingdom)
FEAT	Fair Event Alliance for Ticketing
FSMA	Financial Services and Markets Authority (Belgium)
G2RS	Global Registry and Regulatory Solutions
GASA	Global Anti-Scam Alliance
GLP-1	Glucagon-Like Peptide-1
HPRA	Health Products Regulatory Authority (Ireland)
HTML	Hypertext Markup Language
IC3	Internet Crime Complaint Center
ICC	International Chamber of Commerce
ICO	Initial Coin Offering
IM	Instant Messaging
IOCTA	Internet Organised Crime Threat Assessment
IOSCO	International Organization of Securities Commissions
IPO	Initial Public Offering
IRS	Internal Revenue Service (United States)
ISBN	International Standard Book Number
ISSN	International Standard Serial Number
KYBC	Know Your Business Customer
KYC	Know Your Customer
LMIO	Landelijk Meldpunt Internetoplichting (Dutch National Reporting Centre for Internet Fraud)
MiCA	Markets in Crypto-Assets Regulation
MiFID II	Markets in Financial Instruments Directive II (Directive 2014/65/EU)
NFT	Non-Fungible Token
NIICS	Number-Independent Interpersonal Communication Services

Abbreviation	Full Term
OCC	Oficina de Coordinación de Ciberseguridad (Spanish Cybersecurity Coordination Office)
OECD	Organisation for Economic Co-operation and Development
ÖIAT	Österreichisches Institut für angewandte Telekommunikation (Austrian Institute for Applied Telecommunications)
OJ	Official Journal (of the European Union)
OLAF	Office européen de lutte antifraude (European Anti-Fraud Office)
OSA	Online Safety Act
OSMP	Observatoire de la sécurité des moyens de paiement (French Observatory for Payment Security)
PDF	Portable Document Format
PHAROS	Plateforme d'Harmonisation, d'Analyse, de Recoupement et d'Orientation des Signalements
PSA	Public Service Announcement
SEO	Search Engine Optimisation
SMS	Short Message Service
SoRs	Statements of Reasons
SRA	Systemic Risk Assessment Report
TASC	Tech Against Scams Coalition
TTPA	Transparency of Targeted Political Advertising (Regulation)
UK	United Kingdom
UNIFAB	Union des Fabricants
UNODC	United Nations Office on Drugs and Crime
URL	Uniform Resource Locator
US/U.S.	United States
USD	United States Dollar
VLOP	Very Large Online Platform
VLOSE	Very Large Online Search Engine
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
vzbv	Verbraucherzentrale Bundesverband (Federation of German Consumer Organisations)

Glossary

Term	Explanation
Advance Fee Mechanism	An operational tool whereby victims are required to pay upfront fees (framed as taxes, administrative costs, or processing charges) before receiving a promised benefit that never materialises.
Airdrop Scam	A cryptocurrency fraud exploiting fake free token distributions to trick users into connecting wallets to malicious smart contracts, enabling unauthorised asset transfers.
Algorithmic Amplification	The process by which platform recommendation systems prioritise engaging content, inadvertently surfacing scam material to users through engagement-maximising logic.
Artificial Streaming Scam	Use of automated bots or scripts to artificially inflate engagement metrics on streaming or social media platforms to reach monetisation thresholds or manipulate ranking algorithms. *Note: Also referred to as 'viewbotting' in relation to livestreams or video content.'*
Bait-and-Switch	A deceptive technique where scammers submit legitimate content for platform review, then replace it with fraudulent material once approved. *Note: Also called 'post-approval content switching.'*
Black-hat SEO / SEO Poisoning	Manipulation of search engine optimisation techniques to surface fraudulent pages in organic search results by exploiting ranking algorithms.
Bot Accounts / Bot Networks	Automated accounts used to amplify scam credibility, distribute phishing messages, inflate engagement metrics, or conduct mass outreach.
Charity Scam	Fraudulent scheme exploiting moments of heightened public empathy (disasters, conflicts) by soliciting donations through fake charity organisations or campaigns.
Cloaking / Link Cloaking	Technique serving different content to different users based on identity or device characteristics, showing harmless pages to moderators while redirecting normal users to scam sites.
Counterfeit Products Scam	Sale of fake versions of branded products through online channels, typically at unusually low prices, involving both primary markets (where consumers are deceived) and secondary markets (where consumers knowingly purchase fakes).
Cross-Platform Pathway	The migration pattern by which scams move across different digital environments (e.g., from paid ads to messaging apps to fake websites), exploiting each platform's features at different stages.
Crypto-asset	Digital representation of value or rights transferable and storable electronically using distributed ledger technology or similar systems.
Cryptocurrency Giveaway Scam	Fraud using fake websites and celebrity impersonation to promise doubling of cryptocurrency sent to a scammer-controlled wallet address.

Term	Explanation
Dark Patterns	Deceptive design techniques embedded in platform interfaces that manipulate users into actions they did not intend, such as subscribing or preventing cancellation.
Deepfake	AI-generated or AI-manipulated video, audio, or images used to fabricate or alter the appearance of real individuals, frequently deployed in celebrity endorsement scams.
Designated Service	A platform or search engine designated as a VLOP or VLOSE. *Note: Used as a collective term; sometimes 'VLOPs and VLOSEs' is used interchangeably.*
Digital Services Coordinator (DSC)	National authority responsible for matters relating to the supervision and enforcement of the Digital Services Act in relation to providers established in its Member State, except for the enforcement of the obligations specific to providers of designated services. *Note: See Articles 49-51 and 65 of the Digital Services Act.*
DM to Collab Scam	Fraud targeting content creators through fake sponsorship or collaboration offers sent via direct messages, requiring upfront payments for non-existent partnerships.
Domain name	Human-readable text address used to access websites.
Dynamic Ads	Advertising feature allowing multiple versions of the same campaign simultaneously, exploited by scammers to embed fraudulent ads within legitimate ad sets.
E-commerce Scam	Broad category of fraudulent schemes relying on exchange of goods or services, including fake webshops, counterfeits, undelivered products, and subscription scams.
Employment and Collaboration Scam	Fraudulent schemes where criminals pose as employers or recruiters to deceive victims into believing they have secured legitimate employment opportunities.
Fake Initial Coin Offering (ICO)	Fraudulent fundraising scheme imitating legitimate cryptocurrency token launches to lure investors into purchasing worthless or non-existent coins.
Fake Webshop / Ghost Store	Fraudulent online storefront advertising products at implausibly low prices, collecting payments, then failing to deliver goods. *Note: Both terms are used interchangeably.*
Finfluencer	Individual presenting themselves as a financial advisor or successful investor on social media, often promoting fraudulent investment opportunities through lifestyle content.
Fraud-as-a-Service (FaaS)	Criminal business model where ready-to-use scam tools, infrastructure, and expertise are sold as subscription services, lowering barriers to cybercrime entry.
Friction Tools	Deliberate design interventions introducing pauses, warnings, or confirmation steps to slow harmful or impulsive user behaviour at the point of scam engagement.
Gambling Scam	Fraud involving fake online casinos, betting services, or gaming platforms that manipulate outcomes to prevent genuine payouts.
Ghost Broker	Fraudster posing as a legitimate insurance intermediary, selling fake or invalid insurance policies through social media.
Inherent Risk	The level of risk before mitigation measures are applied; used in platform systemic risk assessments.

Term	Explanation
Infrastructure-as-a-Service (criminal model)	Operational model where a core criminal team manages technical infrastructure while a decentralised network operates individual fraudulent operations on that shared infrastructure.
Intermediary Service	Information society service that transmits, temporarily stores or hosts information provided by its users. *Note: See Article 3(g) Digital Services Act.*
Investment Scam	Fraudulent scheme promising victims significant financial returns through deceptive practices, operating through social media, fake websites, and messaging apps.
Memecoin	Speculative virtual coin originating from internet memes, deriving value from social media promotion rather than underlying utility, often promoted by finfluencers.
Modus Operandi	The operational method or characteristic approach used by scammers to execute a particular type of fraud.
Money Mule	An individual recruited (often unknowingly) to receive and transfer illicit funds through their bank accounts, creating distance between criminal networks and proceeds.
NFT Scam (Non-Fungible Token Scam)	Fraud linked to cryptographic digital assets where projects are promoted then abandoned ('rug pull'), leaving investors unable to recover assets.
NIICS (Number-Independent Interpersonal Communications Services)	Communication services (e.g., WhatsApp, Telegram) that fall outside the DSA regulatory scope but play a critical role in scam operations. *Note: Also referred to as 'private messaging functions.'*
Online Financial Scam	Fraudulent scheme occurring on intermediary services that exploits internet-based anonymity, reach and speed to deceive victims into transferring money, assets, or personal information.
Online Safety Act	UK legislative act that places duties on online platforms and search engines to protect users from illegal and harmful content.
Penny Stock Scam	Manipulation of low-priced shares through misleading promotional campaigns to artificially inflate value before selling at profit.
Phishing	Cyberattack technique enabling the unfair extraction of credentials, personal data or payments through deceitful communications via email, messages, or websites. Variants: spear phishing (targeted), vishing (voice), smishing (SMS).
Phishing-as-a-Service	Commercial toolkits sold by organised crime vendors providing ready-made phishing infrastructure, lowering technical barriers to entry.
Platform Monetisation Systems	Revenue redistribution programmes on social media platforms through which a portion of the advertising or subscription revenue is shared with content creators, based on metrics like views, engagement or subscriber support.
Ponzi Scheme	High-yield investment fraud paying returns from new investor contributions rather than genuine profits, collapsing when recruitment declines.
Pre-IPO Scam	Fraudulent offers to purchase shares in a company before public listing, typically involving misrepresented or fictitious early-stage investment opportunities.

Term	Explanation
Programmatic Advertising	Automated ad placement systems that distribute advertisements at scale, exploited by scammers due to limited oversight of ad content at point of distribution.
Pump-and-Dump Scheme	Coordinated promotion to artificially inflate a crypto-asset's price, followed by mass selling by organisers, causing a sharp price decline for late investors.
Pyramid Scheme	Multi-level fraudulent structure requiring entry fees and recruitment of new members, with returns generated from new contributions.
Recommender System	Algorithmic tool analysing user behaviour and engagement to suggest personalised content, which can inadvertently surface scam material.
Recovery Scam	Secondary fraud targeting previous scam victims by claiming ability to recover lost funds, extracting additional payments.
Residual Risk	The level of risk remaining after mitigation measures are applied; used in platform systemic risk assessments.
Romance Baiting (Pig Butchering / Cryptorom)	Hybrid scam combining prolonged emotional manipulation with fraudulent cryptocurrency investment schemes. *Note: 'Romance baiting,' 'pig butchering,' and 'cryptorom' all refer to the same phenomenon.*
Romance Scam	Fraud constructing fictitious romantic relationships to exploit emotional trust and extract money or personal information from victims.
Rug Pull	Cryptocurrency/NFT scam where a project is heavily promoted then abruptly abandoned by organisers, leaving investors unable to recover assets.
Search Engine Optimisation (SEO)	Techniques for improving website visibility in search results; abused by scammers through poisoning, domain hijacking, and content manipulation.
Sextortion	Coercion and blackmail involving explicit material, where offenders threaten to disclose intimate images unless payment is made.
Shilling Attack / Fake Review Injection	Use of fake reviews to manipulate marketplace recommendation algorithms and promote fraudulent products.
Smart Contract	Self-executing code on a blockchain used in legitimate cryptocurrency operations but exploited by scammers through hidden malicious functions.
Social Engineering	Psychological manipulation techniques designed to exploit cognitive biases, induce vulnerability, and lower victim vigilance.
Spoofing-as-a-Service	Commercial model offering tools for large-scale impersonation of trusted institutions via caller ID manipulation.
Statement of Reasons (SoR)	Formal explanation platforms must provide the following content moderation decisions, recorded in a central transparency repository.
Subscription Scam	Fraud charging victims regularly without genuine consent, using hidden contractual terms, dark patterns, or complex cancellation processes.
Sucker List	List of previous scam victims shared among scammers to enable re-targeting and further victimisation.

Term	Explanation
Typosquatting	Registration of lookalike domain names closely resembling legitimate brands with spelling differences to deceive users.
Unexpected Gain Scam	Fraud based on promises of unanticipated financial rewards or prizes, requiring upfront fees to claim benefits that never materialise.
Very Large Online Platform (VLOP)	Online platform reaching more than 45 million monthly active users in the EU which is subject to enhanced obligations pursuant to a designation decision adopted by the European Commission. *Note: See Article 33 Digital Services Act.*
Very Large Online Search Engine (VLOSE)	Online search engine reaching more than 45 million monthly active users in the EU which is subject to enhanced obligations pursuant to a designation decision adopted by the European Commission. *Note: See Article 33 Digital Services Act.*
VoIP (Voice over Internet Protocol)	Technology enabling voice calls via internet-based networks, exploited by scammers for high-volume calls with location concealment and caller ID spoofing.
Window of Tolerance	Psychological concept referring to the optimal zone of emotional functioning; scams push victims beyond this window into states where critical faculties are compromised.

Abstract

This study supports the European Commission's supervisory work on online financial scams under the Digital Services Act. It examines how scams manifest across designated services, their impact on users and society, and the countermeasures available. It does not assess platform compliance with DSA obligations. Drawing on desk research, stakeholder interviews, a survey of national authorities and a multi-stakeholder workshop, the study develops a typology of six scam categories: investment, romance, e-commerce, employment and collaboration, unexpected gain, and charity and disaster relief. The study analyses the platform features enabling scam dissemination, alongside AI's growing role in scaling deception. Findings indicate substantial economic and social harm, with losses reaching billions of euros annual and significant psychological impacts on victims. To address these risks, the report identifies four categories of countermeasures: access and gatekeeping, detection and removal, user-facing protections, and structural governance and cooperation. The study therefore aims to provide an evidence base to inform ongoing EU regulatory and policy activity addressing online financial scams.

Executive Summary

Background and purpose

Every day, millions of Europeans use online platforms to shop, invest, find work, and connect with others. These services have transformed daily life, but they have also created new opportunities for criminals. Online financial scams – fraudulent schemes whose primary aim is to extract money from victims – have grown into a pervasive crime in the digital age, present across all types of online intermediary services, including Very Large Online Platforms and Very Large Search Engines ('designated services' or 'VLOPs and VLOSEs' hereinafter). Globally, losses from financial scams may now reach as much as **EUR 900 billion each year**.[1] In 2024 alone, more than half of adults worldwide reported encountering at least one scam attempt.[2]

VLOPs and VLOSEs are **systematically misused** for online financial scams. Fraudsters abuse their features to reach users, establish trust, and induce them to disclose personal financial information or make payments. Online financial scams are therefore relevant to the Digital Services Act (DSA) framework, in particular Articles 34 and 35, which require designated services to assess and mitigate systemic risks, including the dissemination of illegal content, and any actual or foreseeable negative effects for the exercise of fundamental rights, including the right to a high-level of consumer protection under Article 38 of the Charter of Fundamental Rights.

Understanding how scams work online, their effects on users and society, and what measures are available to address them is crucial to the implementation of the DSA. However, this study **does not assess or evaluate the compliance of any individual platforms** with their DSA obligations.

Key findings

The study identifies **six broad categories** of online financial scams: investment, romance, e-commerce, employment and collaboration, unexpected gain, and charity and disaster relief scams. Each category encompasses multiple types of scams and has its own distinct characteristics. However, the scam landscape is defined by increasingly overlapping methods.

Of these categories, investment scams (encompassing both traditional and cryptocurrency variants) and e-commerce scams are among the **most common and fastest-growing forms of scams** in Europe. Romance scams also play a notable role in the scam landscape. These categories are briefly introduced below.

Investment scams promise high, guaranteed returns and frequently use deepfake celebrity endorsements, fabricated trading platforms, and private messaging groups to

[1] GASA, Global State of Scams (2025), available at: https://gasa.org/knowledge-base/reports/global-state-of-scams-2025.

[2] ibid.

lure victims. Estimated losses across Europe reached EUR 4 billion in 2024, while global losses linked to cryptocurrency scams alone were estimated at EUR 15 billion in 2025.[3]

Romance scams exploit emotional trust by constructing fictitious personal relationships with users. This category covers a particularly insidious variant, known as “romance baiting”, which combines romantic manipulation with fraudulent cryptocurrency investment. In 2024, romance baiting reports grew by almost 40% year-on-year, reportedly generating between EUR 9.1 billion and EUR 11.4 billion, and accounting for over one-third of global cryptocurrency scam revenue.[4]

E-commerce scams exploit consumers’ expectations of attractive products or services. This is the most heterogeneous category identified, spanning undelivered-product scams, counterfeits, health and wellness scams, rental scams and others. The "BogusBazaar" criminal network illustrates the scale of the threat, operating more than 22,500 fraudulent online stores across Europe between 2021 and 2024.[5]

Perhaps the most significant finding of the study is that **online financial scams are not isolated incidents exploiting peripheral weaknesses**. Scammers operate through the very same advertising systems, recommendation algorithms, account creation processes, monetisation models, and private messaging features that legitimate users rely on every day. To that end, the study posits that the design logic of platforms may create conditions that are inherently conducive to fraudulent activity.

Advertising systems emerged as a primary dissemination channel. Research cited in the study found that nearly **one in three advertisements** on certain major platforms in the EU and UK directed users to **scam, phishing, or malware content**.[6] Recommendation algorithms, designed to surface engaging content, can **amplify scam narratives** framed around urgency and exclusivity before detection systems are triggered. Low-friction account creation processes can enable the **rapid deployment of fake personas** and bot accounts at scale, while private messaging functionalities allow scammers to **groom victims** and migrate them away from public-facing moderation systems.

The boundaries between scam categories are blurring. **Criminals strategically select platforms, exploit trending content, and rapidly adjust their techniques** in response to enforcement actions. This **adaptive behaviour** means that **static, category-based approaches to classification and detection are becoming insufficient**.

Fraudsters now benefit from an industrialised criminal infrastructure. **Fraud-as-a-service** markets offer commercially available deepfake tools, phishing kits, bot networks, and website cloning services, dramatically lowering the barrier to entry. Any actor willing to pay can access the same sophisticated toolkit. If platforms only remove individual

---

[3] Investigate Europe, Scam Europe (2025), available at: https://www.investigate-europe.eu/themes/investigations/-scam-europe; Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/.

[4] Chainalysis, The Rise of Pig Butchering Scams: Revenue Growth and Criminal Ecosystems (2024), available at: https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/.

[5] Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar.

[6] Gen Digital, The Scam Ad Machine (2026), available at: https://www.gendigital.com/blog/insights/research/scam-ad-machine-meta.

fraudulent advertisements, posts, or accounts, the underlying **criminal networks and repeat offenders** that sustain scam campaigns can often remain intact.

The cross-platform nature of scams complicates prevention. Online financial scams rarely remain on a single platform. The study identifies **recurrent migration pathways**: scams typically move from paid advertisements, organic social media content, or search engine results to private messaging applications, and then on to fraudulent external websites. No single platform controls the entire scam chain. Enforcement action on one service may result in displacement, pushing the activity elsewhere. Effective countermeasures must therefore **account for the interconnected ecosystem** through which scams operate.

Artificial intelligence acts as a **transformative amplifier of existing scam methods**. AI-generated deepfakes enable convincing impersonations of celebrities and public figures. Automated social engineering tools can conduct persuasive conversations with multiple victims simultaneously. Multilingual content production allows scams to cross linguistic borders with minimal effort, and real-time adaptation enables scammers to adjust their tactics in response to detection systems. Collectively, these capabilities are shifting the balance of advantage further towards criminal operators.

In response to the risks, the study maps **countermeasures across four categories**: access and gatekeeping measures (identity verification, advertiser vetting, AI-content labelling); detection and removal measures; user-facing protections (reporting tools, redress information, friction tools); and structural governance (platform policies, third-party cooperation).

Access and gatekeeping measures represent the first line of defence against online financial scams by controlling who and what can reach users on a platform. **Detection and removal measures** cover automated detection, human review, removal/suspension mechanisms, detection of coordinated scam networks, and recommender-system protection measures. Their objective is to identify and neutralise scam content and actors once they are present on a platform. **User-facing measures** operate at the point of interaction between platform and end user, equipping users with tools and information to identify, report, and resist online financial scams. Last, **platform-level policies and cooperation with third parties** encompass the foundational rules and institutional frameworks through which platforms define, prevent, and address online financial scams. They shape all downstream detection, moderation, and enforcement activities.

Several **important gaps emerge**. High-assurance identity verification of advertisers before they can place advertisements remains the exception rather than the rule, as most platforms rely on self-declaration. Stronger mandatory verification has been introduced i.a. in Singapore and Taiwan. As a result, scam advertisements fell by between 29% and 96%, suggesting that more rigorous gatekeeping could yield significant results.[7] Detection efforts remain focused on individual content items rather than on the coordinated networks behind them. Stakeholders also claim there are notable discrepancies between the formal policy rules that platforms publish and the actual moderation outcomes observed in practice.

Overall, while designated services have developed a wide range of gatekeeping, detection, user-facing and structural countermeasures, the evidence reviewed points to remaining avenues for improvement. Stakeholders and third-party research consistently

[7] Reuters, Meta created 'playbook' to fend off pressure to crack down on scammers, documents show (2026), available at: https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/.

recommend a **shift towards network-level and infrastructure-level disruption**, **stronger and more consistently applied verification** at points of high risk (advertising, regulated sectors), and **closer cross-sector and cross-border cooperation** between platforms, financial institutions, telecommunications providers and law enforcement.

Social and Economic Impact

The scale of online financial scams is substantial, although available data are likely to **underestimate the true extent of victimisation and harm** because many incidents are not reported.

The harm caused by online financial scams **extends far beyond the immediate monetary loss.** As mentioned above, global estimates suggest losses of up to EUR 0.9 trillion annually. Yet the true figures are almost certainly higher, given that the vast majority of victims never report the crime.

The **social and psychological consequences** are equally severe. Research shows that 79% of scam victims report emotional harm, including irritation, anger, stress, and embarrassment.[8] Many victims change their online behaviour after an experience with fraud: 34% altered how they use the internet, while 28% reported a lasting loss of trust.[9] Moreover, shame and fear of judgement discourage reporting and expose victims to secondary victimisation and re-victimisation through 'recovery scams'. These are fraudulent schemes that target people who have already lost money to a previous scam, falsely promising to recover their lost funds for an upfront fee.

These burdens **fall disproportionately on those who are already vulnerable**: financially insecure individuals, people experiencing loneliness, younger users drawn to speculative digital environments, and older adults with limited digital literacy. At a market level, 53% of victims of online buying scams changed their purchasing behaviour afterwards, pointing to a broader erosion of consumer trust in digital commerce that threatens the functioning of the EU's internal market.[10]

Looking ahead

This study provides a comprehensive mapping of the online financial scam landscape on platforms as it stands in 2026. The picture that emerges is one of a phenomenon deeply embedded in the architecture of digital platforms, increasingly industrialised in its operational infrastructure, and growing in both its economic and human toll. Significant evidence gaps remain: the true prevalence of scams across the EU is unknown in the absence of harmonised data collection; the causal relationship between recommendation algorithms and scam amplification has not been empirically established at scale; and the effectiveness of individual countermeasures remains largely unquantified.

[8] European Commission, Study on online identity theft and identity related crime – Final report (2022), available at: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1/language-en.

[9] European Union Agency for Fundamental Rights, Online fraud – people's experiences across the EU (2026), available at: https://fra.europa.eu/en/publication/2026/victims-online-fraud.

[10] ibid.

The findings underline the need for sustained, evidence-based, and coordinated action across platforms, regulators, law enforcement, and civil society that addresses not only the symptoms of online financial scams but also the structural conditions that enable them to persist and proliferate.

Synthèse

Contexte et objectif

Chaque jour, des millions d'Européens utilisent des plateformes en ligne pour faire des achats, investir, trouver un emploi et communiquer avec d'autres personnes. Ces services ont transformé la vie quotidienne, mais ils ont également créé de nouvelles possibilités pour les criminels. Les arnaques financières en ligne – des stratagèmes frauduleux dont l'objectif principal est de soutirer de l'argent à leurs victimes – constituent désormais un fléau omniprésent à l'ère numérique, qui touche tous les types de services intermédiaires en ligne, y compris les très grandes plateformes en ligne et les très grands moteurs de recherche en ligne (ci-après les « services désignés » ou les « VLOPs et VLOSEs »). À l'échelle mondiale, les pertes dues aux arnaques financières pourraient désormais atteindre **900 milliards d'euros par an**.[11] En 2024 seulement, plus de la moitié des adultes dans le monde ont déclaré avoir été confrontés à au moins une tentative d'arnaque.[12]

Les VLOPs et VLOSEs sont **systématiquement détournés** pour mener des arnaques financières en ligne. Les fraudeurs détournent leurs fonctionnalités pour atteindre les utilisateurs, instaurer un climat de confiance et les inciter à divulguer des informations financières personnelles ou à effectuer des paiements. Les arnaques financières en ligne entrent donc dans le cadre du règlement sur les services numériques (DSA), en particulier ses articles 34 et 35, qui imposent aux services désignés d'évaluer et d'atténuer les risques systémiques, tels que la diffusion de contenus illicites, ainsi que tout effet négatif réel ou prévisible sur l'exercice des droits fondamentaux, y compris le principe d'un niveau élevé de protection des consommateurs prévu à l'article 38 de la Charte des droits fondamentaux.

Il est essentiel, pour mettre en œuvre le DSA, de comprendre le fonctionnement des arnaques en ligne, leurs effets sur les utilisateurs et la société, ainsi que les mesures disponibles pour y faire face. Toutefois, la présente étude **n'évalue ni n'apprécie le respect, par une quelconque plateforme, de ses obligations au titre du DSA**.

Principales conclusions

L'étude recense **six grandes catégories** d'arnaques financières en ligne : investissement, arnaques sentimentales, arnaques liées au commerce en ligne, arnaques liées aux collaborations commerciales et partenariats rémunérés, arnaques aux gains inattendus, et arnaques liées aux œuvres caritatives et à l'aide aux victimes de catastrophes. Chaque catégorie englobe plusieurs types d'arnaques et possède ses propres caractéristiques. Toutefois, le paysage des arnaques se caractérise par des méthodes qui se recoupent de plus en plus.

Parmi ces catégories, les arnaques à l'investissement (y compris les variantes traditionnelles et celles liées aux cryptomonnaies) et les arnaques liées au commerce en ligne comptent parmi les **formes d'arnaque les plus courantes et à la croissance**

[11] GASA, Global State of Scams (2025), available at: https://gasa.org/knowledge-base/reports/global-state-of-scams-2025.

[12] ibid.

la plus rapide en Europe. Les arnaques sentimentales jouent également un rôle important dans le paysage des arnaques. Ces catégories sont présentées brièvement ci-dessous.

Les arnaques à l'investissement promettent des rendements élevés et garantis et recourent fréquemment à de fausses recommandations de célébrités réalisées au moyen de deepfakes, à des plateformes d'investissement fictives et à des groupes de messagerie privée pour attirer les victimes. Les pertes estimées à travers l'Europe ont atteint 4 milliards d'euros en 2024, tandis que les pertes mondiales liées aux seules arnaques aux cryptomonnaies étaient estimées à 15 milliards d'euros en 2025.[13]

Les arnaques sentimentales exploitent la confiance affective en nouant des relations personnelles fictives avec les utilisateurs. Cette catégorie couvre une variante particulièrement insidieuse, connue sous le nom de « romance baiting », qui associe manipulation sentimentale et investissement frauduleux dans les cryptomonnaies. En 2024, le nombre de signalements de romance baiting a augmenté de près de 40 % par rapport à l'année précédente ; selon les informations disponibles, cette pratique aurait généré entre 9,1 milliards d'euros et 11,4 milliards d'euros et représenté plus d'un tiers des revenus mondiaux issus des arnaques aux cryptomonnaies.[14]

Les arnaques liées au commerce en ligne exploitent les attentes des consommateurs à l'égard de produits ou de services attractifs. Il s'agit de la catégorie recensée la plus hétérogène; elle englobe les arnaques liées à des produits non livrés, les contrefaçons, les arnaques dans les domaines de la santé et du bien-être, les arnaques à la location et d'autres encore. Le réseau criminel « BogusBazaar » illustre l'ampleur du danger : il a exploité plus de 22 500 boutiques en ligne frauduleuses dans toute l'Europe entre 2021 et 2024.[15]

L'une des conclusions les plus importantes de l'étude est que les arnaques financières en ligne **ne sont pas des incidents isolés qui exploitent des vulnérabilités périphériques**. Les arnaqueurs opèrent au moyen des mêmes systèmes publicitaires, algorithmes de recommandation, processus de création de comptes, modèles de monétisation et fonctionnalités de messagerie privée sur lesquels les utilisateurs normaux s'appuient chaque jour. À cet égard, l'étude avance que la logique de conception des plateformes peut créer des conditions intrinsèquement propices aux activités frauduleuses.

Les systèmes publicitaires sont apparus comme un canal de diffusion principal. Les recherches citées dans l'étude ont révélé que près d'**une publicité sur trois** diffusée sur certaines grandes plateformes dans l'UE et au Royaume-Uni redirigeait les utilisateurs vers des **contenus liés à des arnaques, à du hameçonnage ou à des logiciels malveillants**.[16] Les algorithmes de recommandation, conçus pour mettre en

[13] Investigate Europe, Scam Europe (2025), available at: https://www.investigate-europe.eu/themes/investigations/-scam-europe; Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/.

[14] Chainalysis, The Rise of Pig Butchering Scams: Revenue Growth and Criminal Ecosystems (2024), available at: https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/.

[15] Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar.

[16] Gen Digital, The Scam Ad Machine (2026), available at: https://www.gendigital.com/blog/insights/research/scam-ad-machine-meta.

avant des contenus suscitant l'engagement, peuvent **amplifier les récits d'escroquerie** fondés sur l'urgence et l'exclusivité avant que les systèmes de détection ne soient déclenchés. Les processus de création de comptes peu exigeants peuvent permettre le **déploiement rapide de fausses identités** et de comptes automatisés à grande échelle, tandis que les fonctionnalités de messagerie privée permettent aux escrocs de **gagner la confiance des victimes** et de les éloigner des systèmes de modération des espaces publics.

Les frontières entre les catégories d'arnaques s'estompent. Les criminels sélectionnent stratégiquement les plateformes, exploitent les contenus en vogue et adaptent rapidement leurs techniques en réaction aux mesures de contrôle. Cette **capacité d'adaptation** signifie qu'en matière de classification et de détection, les approches statiques et fondées sur les catégories deviennent insuffisantes.

Les fraudeurs bénéficient désormais d'une infrastructure criminelle industrialisée. Les marchés de **fraude en tant que service** proposent des outils de deepfake disponibles dans le commerce, des kits d'hameçonnage, des réseaux de robots et des services de clonage de sites web, ce qui abaisse considérablement le seuil d'entrée. Tout acteur prêt à payer peut accéder au même arsenal sophistiqué. Si les plateformes se contentent de supprimer des publicités, des publications ou des comptes frauduleux pris individuellement, les **réseaux criminels et récidivistes** derrière les campagnes d'escroquerie peuvent souvent rester intacts.

La dimension interplateforme des arnaques complique la prévention. Les arnaques financières en ligne restent rarement cantonnées à une seule plateforme. L'étude recense des **trajectoires de migration récurrentes** : les arnaques passent généralement de publicités payantes, de contenus organiques sur les réseaux sociaux ou de résultats de moteurs de recherche à des applications de messagerie privée, puis à des sites web externes frauduleux. Aucune plateforme ne contrôle à elle seule l'ensemble de la chaîne d'exécution de l'arnaque. Une mesure de contrôle visant un service peut entraîner un déplacement de l'activité, qui se reporte ailleurs. Les contre-mesures efficaces doivent donc **tenir compte de l'écosystème interconnecté** dans lequel les arnaques opèrent.

L'intelligence artificielle agit comme un **amplificateur qui transforme en profondeur les méthodes d'arnaque existantes**. Les deepfakes générés par l'IA permettent d'imiter de manière convaincante des célébrités et des personnalités publiques. Les outils automatisés d'ingénierie sociale peuvent mener des conversations persuasives avec plusieurs victimes en même temps. La production de contenus multilingues permet aux arnaques de franchir les frontières linguistiques avec peu d'efforts, et l'adaptation en temps réel permet aux escrocs d'ajuster leurs tactiques en réaction aux systèmes de détection. Prises ensemble, ces capacités font pencher davantage la balance au profit des acteurs criminels.

En réponse à ces risques, l'étude recense des **contre-mesures réparties en quatre catégories** : mesures d'accès et de filtrage (vérification de l'identité, contrôle préalable des annonceurs, étiquetage des contenus générés par l'IA) ; mesures de détection et de retrait ; protections destinées aux utilisateurs (outils de signalement, informations sur les voies de recours, outils de friction) ; et gouvernance structurelle (politiques des plateformes, coopération avec des tiers).

Les **mesures d'accès et de filtrage** constituent la première ligne de défense contre les arnaques financières en ligne, en contrôlant les acteurs et les contenus susceptibles d'atteindre les utilisateurs sur une plateforme. Les **mesures de détection et de retrait** comprennent la détection automatisée, l'examen humain, les mécanismes de retrait ou de suspension, la détection des réseaux d'arnaque coordonnés et les mesures de

protection des systèmes de recommandation. Leur objectif est d'identifier et de neutraliser les contenus et les acteurs liés aux arnaques dès lors qu'ils sont présents sur une plateforme. Les **mesures destinées aux utilisateurs** interviennent au point d'interaction entre la plateforme et l'utilisateur final, en dotant les utilisateurs d'outils et d'informations pour identifier, signaler et contrer les arnaques financières en ligne. Enfin, les **politiques au niveau des plateformes et la coopération avec des tiers** englobent les règles fondamentales et les cadres institutionnels par lesquels les plateformes définissent, préviennent et traitent les arnaques financières en ligne. Elles façonnent toutes les activités ultérieures de détection, de modération et de contrôle.

Plusieurs lacunes importantes apparaissent. La vérification approfondie de l'identité des annonceurs avant de les autoriser à diffuser des publicités reste l'exception plutôt que la règle, la plupart des plateformes s'appuyant sur une simple autodéclaration. Des obligations de vérification plus strictes ont notamment été introduites à Singapour et à Taïwan. En conséquence, le nombre de publicités frauduleuses a diminué de 29 % à 96 %, indiquant qu'un filtrage plus rigoureux pourrait produire des résultats significatifs.[17] Les efforts de détection restent axés sur les contenus pris individuellement plutôt que sur les réseaux coordonnés qui les sous-tendent. Les parties prenantes affirment également qu'il existe des divergences notables entre les règles officielles publiées par les plateformes et les résultats de modération effectivement observés dans la pratique.

Dans l'ensemble, bien que les services désignés aient mis au point un large éventail de contre-mesures en matière de filtrage, de détection et de protection des utilisateurs ainsi que des mesures structurelles, les éléments examinés indiquent des voies d'amélioration. Les parties prenantes et les travaux de recherche menés par des tiers recommandent systématiquement une **évolution vers la neutralisation des réseaux et des infrastructures**, une **vérification plus rigoureuse et appliquée de manière plus cohérente** aux points présentant un risque élevé (publicité, secteurs réglementés), ainsi qu'une **coopération intersectorielle et transfrontière plus étroite** entre les plateformes, les institutions financières, les fournisseurs de télécommunications et les services de police.

Impact social et économique

L'ampleur des arnaques financières en ligne est considérable, bien que les données disponibles soient susceptibles de **sous-estimer la véritable ampleur des agressions et des préjudices**, car de nombreux incidents ne sont pas signalés.

Le préjudice causé par les arnaques financières en ligne **va bien au-delà de la perte financière immédiate**. Comme indiqué ci-dessus, les estimations mondiales font état de pertes pouvant atteindre 900 milliards d'euros par an. Cependant, les chiffres réels sont presque certainement plus élevés, étant donné que la grande majorité des victimes ne signalent jamais l'infraction.

Les **conséquences sociales et psychologiques** sont tout aussi graves. Les recherches montrent que 79 % des victimes d'arnaques font état d'un préjudice

[17] Reuters, Meta created 'playbook' to fend off pressure to crack down on scammers, documents show (2026), available at: https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/.

émotionnel, notamment de l'agacement, de la colère, du stress et de la gêne.[18] De nombreuses victimes modifient leur comportement en ligne après avoir été victimes d'une fraude : 34 % ont changé leur manière d'utiliser internet, tandis que 28 % font état d'une perte de confiance durable.[19] En outre, la honte et la crainte du jugement dissuadent les victimes de signaler les faits et les exposent à une victimisation secondaire et à une revictimisation par le biais d'« arnaques au recouvrement ». Il s'agit de stratagèmes frauduleux qui ciblent des personnes ayant déjà perdu de l'argent dans une arnaque antérieure, en leur promettant à tort de récupérer leurs fonds perdus contre le paiement préalable de frais.

Ces conséquences **pèsent de manière disproportionnée sur les personnes déjà vulnérables** : les personnes en situation de précarité financière, les personnes confrontées à la solitude, les utilisateurs plus jeunes attirés par des environnements numériques spéculatifs et les personnes plus âgées ayant une culture numérique limitée. À l'échelle du marché, 53 % des victimes d'arnaques liées aux achats en ligne ont modifié leur comportement d'achat par la suite, ce qui témoigne d'une érosion plus large de la confiance des consommateurs dans le commerce en ligne qui menace le fonctionnement du marché intérieur de l'UE.[20]

Perspectives

La présente étude propose une cartographie complète du paysage des arnaques financières en ligne sur les plateformes tel qu'il se présente en 2026. Le tableau qui se dégage est celui d'un phénomène profondément ancré dans l'architecture des plateformes numériques, dont l'infrastructure opérationnelle est de plus en plus industrialisée et dont le bilan économique et humain ne cesse d'augmenter. D'importantes lacunes en matière de données probantes subsistent : l'ampleur réelle des arnaques à travers l'UE demeure inconnue en l'absence d'une collecte de données harmonisée ; le lien de causalité entre les algorithmes de recommandation et l'amplification des arnaques n'a pas été établi empiriquement à grande échelle ; et l'efficacité de chaque contre-mesure demeure largement non quantifiée.

Les résultats soulignent la nécessité d'une action soutenue, coordonnée et fondée sur des données probantes, associant les plateformes, les autorités de régulation, les services de police et la société civile, afin de s'attaquer non seulement aux symptômes des arnaques financières en ligne, mais également aux facteurs structurels qui favorisent leur persistance et leur prolifération.

[18] European Commission, Study on online identity theft and identity related crime – Final report (2022), available at: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1/language-en.

[19] European Union Agency for Fundamental Rights, Online fraud – people's experiences across the EU (2026), available at: https://fra.europa.eu/en/publication/2026/victims-online-fraud.

[20] ibid.

1. Introduction

1.1. Study objectives and scope

The general aim of this study is to **support the European Commission in its supervisory and analytical activities** in relation to the risks posed by online financial scams across designated services in the context of the Digital Services Act (Regulation (EU) 2022/2065 or DSA). In particular, the study seeks to contribute to the Commission's understanding of **how different types of online financial scams manifest across platforms**, how these scams affect users and society, and how online platforms seek to prevent and address deceptive practices. **The study does not assess or evaluate the compliance of any online platforms or online search engines with the obligations they incur under the DSA.**

In light of this general objective, the study pursues three specified objectives:

- To develop a structured typological mapping of online financial scams present on designated services, including an assessment of their prevalence, emerging trends, and social and economic impacts;
- To map and analyse the strategies, tools, and practices implemented by online platforms as a counterresponse to the presence of online financial scams on their services;
- To explore selected scam typologies and platform contexts in greater depth through targeted case studies.

The context of this study is marked by the entry into full application of the DSA, and the subsequent designation of Very Large Online Platforms (VLOPs) and Very Large Search Engines (VLOSEs). The DSA came into force to regulate online intermediaries and platforms, including marketplaces (such as app stores and online travel and accommodation platforms), social networks, and content-sharing platforms. Overall, the DSA started applying to all concerned services on 17 February 2024. Provisions concerning VLOPs and VLOSEs were included to ensure greater accountability and transparency, outlining additional obligations for the providers of such services. The rules for VLOPs and VLOSEs start applying four months after their designation.

Online financial scams have become increasingly sophisticated, adaptive and cross-platform, often exploiting platform features such as advertising and recommender systems. It is indeed recognised that technological advancement acts as an enabler of increasingly sophisticated financial scam methods and approaches. According to Interpol's Global Financial Fraud Assessment, member countries expect the scope of financial scams to increase, as globalisation and technological development grow.[21] These developments pose significant risks to consumer protection and trust in digital services, rendering DSA rules aimed at enhancing platform accountability and risk mitigation essential.

VLOPs and VLOSEs incur responsibilities directly relevant to combating online financial scams. Article 34 of the DSA requires designated service providers to periodically

[21] Interpol, Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology.

evaluate how the functioning, design, or use of their services might give rise to systemic risks. Two of the risk areas laid out in Article 34 are particularly relevant in this context:

- The dissemination of illegal content under Article 34(1)(a), which encompasses fraudulent content;
- Any negative effect on fundamental rights (Article 34(1)(b), including the principle of a high level of consumer protection enshrined in Article 38 of the EU Charter of Fundamental Rights.[22]

This risk assessment framework lays the foundation for the risk mitigation obligations set in Article 35, requiring platforms to put in place reasonable, effective, and proportionate measures to tackle the identified risks.

Within this context, the study provides an analytical and evidence-based examination of online financial scams and platform practices. It aims to deliver a coherent knowledge base to support ongoing and future regulatory, supervisory, and policy activities related to online financial scams.

1.2. Methodological approach and report structure

To achieve the objectives of the study, the findings were informed by a multi-method approach that included extensive desk research, interviews with stakeholders, a survey with national authorities, and a workshop.

Before providing a detailed overview of the methodology, it is important to acknowledge its potential limitations. Except for input gathered through the stakeholder consultation, **the findings rely on publicly available data**. While this approach ensures traceability, it also **narrows the evidence bank available**. Moreover, because **online financial scams are frequently under-reported**, existing data on their prevalence and impact captures **only a partial picture of the phenomenon**. To address these limitations, data were triangulated wherever possible, cross-checking sources to validate findings. Nonetheless, the findings presented in this report should be interpreted in light of these constraints.

Desk research

The study team conducted extensive and in-depth research to collect information on the typologies of online financial scams, operational characteristics, impact, and countermeasures deployed by online platforms.

As a first step, the study team compiled a repository of sources, drawing from a wide range of EU, international, and national materials. This included publications from EU, international, and national institutions and agencies, academic research, Trusted Flaggers reports, conference papers, reports from civil society and consumer organisations, press releases, news articles, industry publications, and publicly available documentation shared by VLOPs and VLOSEs pursuant to their transparency obligations under the DSA.

The subsequent desk research was guided by a pre-defined framework designed to ensure consistency and alignment with the study objectives. Sources were reviewed and

[22] European Union, Charter of Fundamental Rights of the European Union (2012), available at: https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng.

categorised according to the type of financial scam, the operational models used, the dissemination channels involved, the categories of the affected users, and the types of harm identified. This structured approach supported the identification of recurring patterns and similarities, allowing the detection of emerging scam typologies and tactics. The desk research covered more than 400 sources; those which are explicitly referenced in this Report are listed in Annex I.

Stakeholder consultation

Desk-based findings were complemented by targeted stakeholder consultation activities: interviews, a survey and a multi-stakeholder workshop.

The study team conducted fifteen structured interviews overall, with a selection of stakeholders representing different perspectives on online financial scams. These included EU institutions and agencies, consumer organisations, civil society actors, trusted flaggers, and industry actors. The table below lists the relevant stakeholders interviewed, whereas the interview guides are available in Annex II and III.

Table 1 - Number and type of stakeholders interviewed

Organisation type	Total
Civil Society Organisation	2
Consumer organisation	2
European institution	5
Industry	3
Trusted Flagger	3

Moreover, the study team reviewed and incorporated the responses to the Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”, which was circulated to the Task Force on Online Scams and Fraud by DG CONNECT. This survey targeted a broad range of national authorities, including law enforcement, national Digital Services Coordinators, and regulatory agencies with direct experience with online financial scams. The survey collected responses from 16 Member States, often with multiple national authorities from each Member State providing input.

Lastly, a multi-stakeholder workshop was organised as part of the study to facilitate dialogue among key stakeholders and to gather feedback on the study’s findings and case studies. The full workshop report is available in Annex IV.

The workshop brought together representatives from national authorities, trusted flaggers, and industry actors. It featured guided discussions structured around the study’s principal findings and the case studies. The study team presented the findings to participants, who were subsequently invited to comment and share their observations.

The input received from stakeholders during the workshop was used to further inform and validate the analysis presented in this report. This consultative process ensured that the study’s conclusions were tested against the practical experience and expertise of a diverse range of actors engaged in combating online financial scams.

Analysis

The triangulation of desk research and stakeholder consultation data informed the findings of the present Report, which is structured as follows: the first section is dedicated to the classification of online financial scams (see Section 2); then, the risk factors on designated services and the methods or tools used by scammers are presented (see Section 3), followed by an analysis of the social and economic impact of online financial scams, in terms of the categories of victims and the economic and social harm inflicted (see Section 4). The next section analyses the countermeasures against online financial scams, relying on stakeholder data and on publicly available reports from the designated services (Section 5). Lastly, the findings of the four in-depth case studies carried out by the study team are presented (Section 6), followed by the conclusions (Section 7) and the annexes (Section 8).

2. Typological mapping of online financial scams

In the context of this study, 'online financial scams' are defined as online fraudulent behaviours whose primary objective is to extract a form of financial gain, and which have negative financial consequences for the victims. This distinguishes the scope of the study from scams whose principal target is a financial institution rather than a consumer. This delineation has also been recommended and highlighted by participants to the workshop organised by the study team.[23]

In developing the classification of online financial scams below, the study team assessed the existing typologies of financial scams, as proposed by national authorities, academia or industry. These sources include reports from the European Union Agency for Cybersecurity (ENISA), the European Banking Authority (EBA), Europol, the Australian National Anti-Scam Centre, the UK Financial Conduct Authority, the Global Anti-Scam Alliance, and the UK National Fraud Authority.[24]

By triangulating these sources, the study team has identified the most common types of online financial scams and developed its own typological classification of online financial scams, focusing on fraudulent behaviours which occur on intermediary services, within the meaning of the DSA. Scams solely operationalised through other mediums which fall outside the scope of the DSA (e.g. SMS, phone calls) were explicitly not included. However, because such channels may still influence scam dynamics on designated services (e.g. phishing), they are referenced where relevant to provide a contextual base.

The result of this exercise is a typology structured around six broad groups of online financial scam types: investment scams, romance scams, e-commerce scams, employment and collaboration scams, unexpected gain scams, and charity and disaster relief scams.

For each of these groups, the following sections provide a general description of the types of financial scams they contain, including an analysis of the elements that distinguish a specific type of financial scam from the others, their modus operandi, and the offender profile. In addition, each section provides an initial description of the relation

[23] Multi-stakeholder Workshop on Online Financial Scams.

[24] ENISA, ENISA Threat Landscape 2025 (2026), available at: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf; European Banking Authority, EBA Opinion on new types of payment fraud and possible mitigants (2024), available at: https://eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf; Europol, Europol Spotlight – Online fraud schemes: a web of deceit (2023); https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023; Europol, Internet Organised Crime Threat Assessment 2025 (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf; Europol, Serious and organised crime threat assessment – The changing DNA of serious and organised crime (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf; Australian National Anti-Scam Centre, Targeting Scams – Report of the National Anti-Scam Centre on scams data and activity 2025 (2026), available at: https://www.nasc.gov.au/system/files/targeting-scams-report-2025.pdf; UK Financial Conduct Authority, Protect yourself from scams (2026), available at: https://www.fca.org.uk/consumers/protect-yourself-scams; Global Anti-Scam Alliance, Global State of Scams – 2025 (2025), available at: https://gasa.org/knowledge-base/reports/global-state-of-scams-2025; UK National Fraud Authority, Fraud typologies and victims of fraud – Literature review (2009), available at: https://assets.publishing.service.gov.uk/media/5a7ad8c2ed915d670dd7efad/fraud-typologies.pdf.

between the scam and the environment of designated services and their features, as a primer for the exploration of platform-specific features under Section 3.1.[25]

Any potential divergences from this structure should be understood as resulting from **gaps in the publicly available literature**. As highlighted in the written contributions from participants to the workshop, **victims of online scams often feel shame, making them less likely to report**, which in turn limits the evidence available to media.[26] **Under-reporting directly impacts the availability of data and the understanding of the phenomenon**, which is reflected in the extent of the analysis for certain types of online scams.

The table below presents the types of online financial scams identified as part of this study, their operational model, the risk factors on designated services that facilitate their dissemination, and the tools and techniques used by scammers. The subsequent figure links the types of online financial scams to the relevant risk factors and countermeasures. These are then described in the following paragraphs and in Sections 3 and 5 of this Report.

[25] As a disclaimer, recurrent mentions of a specific VLOP or VLOSE should not be understood as evidence of a higher prevalence of financial scam content on that service. There is limited evidence on this phenomenon unfolding on some VLOPs or VLOSEs, *inter alia*, due to limited access to research data, or due to the limited functionality of their ad libraries. A lack of information should not be conflated with the finding that online financial scams do not occur on those services.

[26] Multi-stakeholder Workshop on Online Financial Scams.

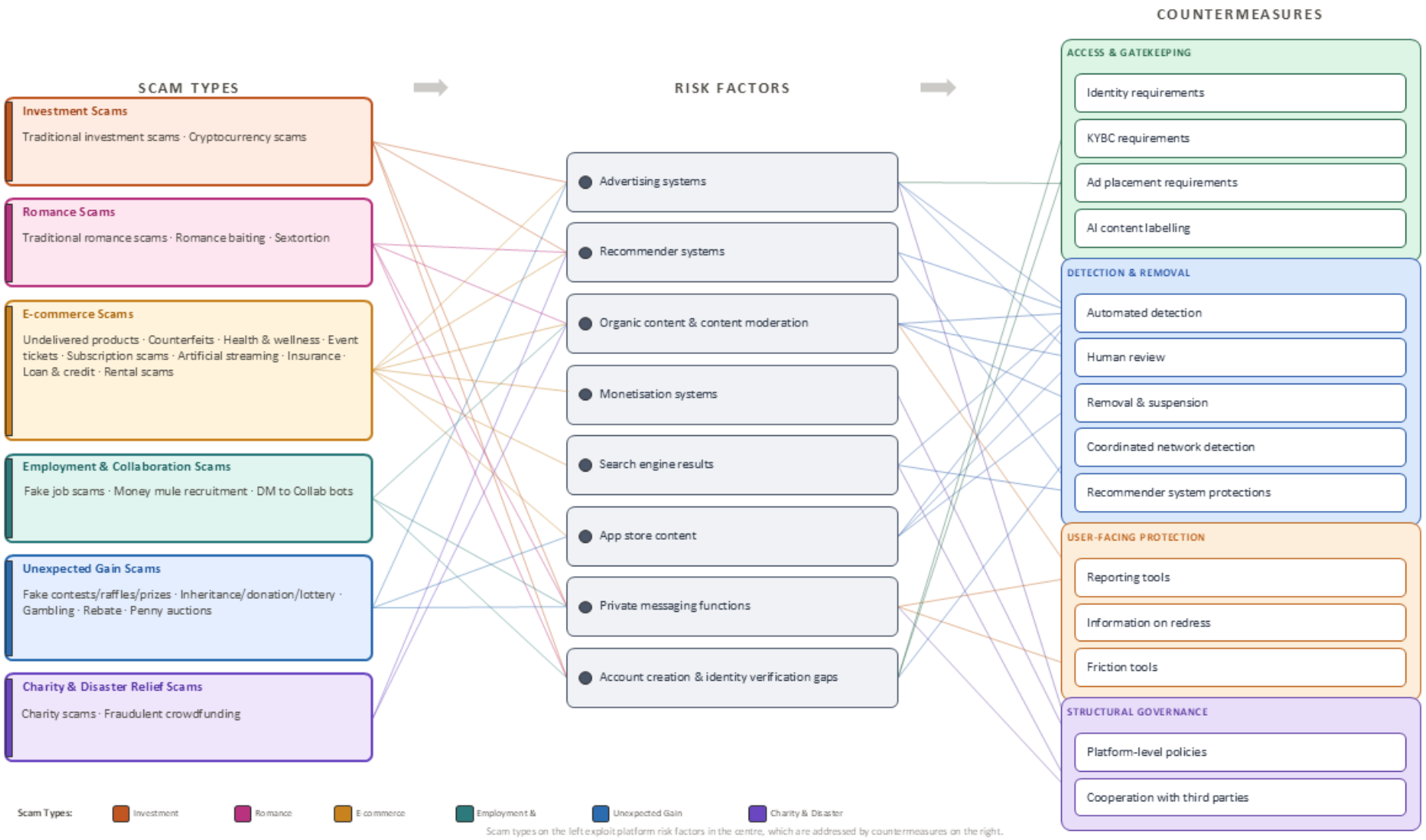
Table 2 - Typological overview of online financial scams

Category	Type of Scam	Operational Model	Risk Factors on Designated Services	Tools & Techniques
Investment Scams	**Traditional investment scams**	Promises high, guaranteed returns that never materialise; victims may earn small returns first to encourage higher investment.	Paid ad systems amplify reach of unauthorised investment services; recommendation algorithms resurface scam profiles and scam content; influencer-fuelled retail demand; private messaging (1-on-1 or in groups) manufacture legitimacy.	Fake trading platforms with fabricated profit dashboards; deepfake celebrity endorsements; WhatsApp/Telegram 'investor community' groups with fabricated proof of earnings and coordinated testimonials.
	Cryptocurrency scams	Fraudsters exploit the volatility and pseudonymous, hard-to-trace nature of crypto-assets across a wide range of subtypes, promising high, guaranteed returns.	Paid ads; recommendation algorithms amplifying urgency/exclusivity; 'finfluencer' content and social media-driven promotion; private messaging (1-on-1 or in groups) for social proof; low barriers to account creation allow bot-amplified engagement.	Fake ads redirecting to spoofed trading platforms, exchanges and wallets; deepfake technology and AI-generated content impersonating trusted individuals or organisations; fraudulent WhatsApp communities built to gradually establish trust; malicious smart contracts enabling unauthorised transfers; manipulative narratives around 'AI trading bots'.
Romance Scams	**Traditional romance scams**	Scammer builds a fake romantic profile, grooms the victim emotionally over time, then requests money for fabricated emergencies.	Low account-creation barriers and limited ID verification enable fake personas; algorithms surface profiles to vulnerable users; social media networking functions (friend requests, likes, comments, reactions) facilitate contact with the victim; private messaging functions allow grooming.	Stolen or fabricated photos and biographies; migration to private chat (WhatsApp/Telegram); 'sucker lists' for re-victimisation; social engineering and psychological manipulation.
	Romance baiting	Combines emotional manipulation with a fraudulent (crypto) investment 'recommendation' introduced after months of relationship-building.	Same features as romance and investment scams combined: recommendation systems, low verification, private-messaging migration.	Prolonged relationship-building scripts; fraudulent investment platforms/dashboards.
	Sextortion	Offenders obtain, or claim to possess, intimate images/videos and extort payment under threat of exposure.	Direct messaging and easy fake-account creation enable coercive contact.	False identities; stolen or fabricated intimate content used as bait; threats of disclosure; coerced content production.
E-commerce Scams	**Undelivered products**	Fraudulent storefronts collect advance payment at implausibly low prices, then disappear without delivering.	Ad systems can't distinguish fraudulent from legitimate campaigns; search engine indexing and ranking systems surface fake stores organically.	Infrastructure-as-a-service; urgency design (countdown/limited-stock signals); credit-card harvesting via spoofed payment interfaces; peak-season targeting (Black Friday, Christmas).
	Counterfeit products	Fake webshops sell counterfeits as genuine ('primary market') or openly as replicas ('secondary market') at low prices.	Social media ads/content sharing, ephemeral content (stories/live broadcasts) limits detection window; ad systems allow scaled targeted promotion; hidden links on marketplaces.	'Dupe'/'clone' keyword evasion of detection systems; dark patterns and fake reviews; DMs for discreet sales.
	Health and wellness scams	Sell unregulated medicines/wellness products via false health claims, exploiting anxiety around medical conditions.	Self-declared advertiser identity abused for anonymity; hyperlink-editing features mislead users to fake sites; algorithmic personalisation targeting health interests.	Deepfakes impersonating health authorities/celebrities; AI-generated 'before/after' imagery; influencer promotion; impersonation of health authorities; manipulated reviews.
	Event ticket scams	Sell tickets for sold-out events that never arrive, or that are fake/stolen, exploiting scarcity and resale demand.	Sponsored search placements outrank official sellers; fake profiles/groups/comment sections on event posts; weak moderation of comments/groups on social media.	Impersonation of official sellers; fake ticket sale webpages; high-price resale exploitation; migration to private messaging to close the sale.
	Subscription scams and hidden renewals	Recurring charges via unclear free-trial terms, hidden contract clauses, near-impossible cancellation paths.	Dark patterns embedded directly in legitimate or fraudulent platform interfaces; sponsored search ads surfacing scam subscription websites.	Confusing/guilt-based cancellation prompts; complicated terms and conditions or hidden information.
	Artificial streaming scams	Automated bots/scripts inflate engagement (views, likes, followers) to unlock performance-based monetisation or boost ranking.	Performance-based monetisation models incentivise inauthentic engagement; recommender systems are gamed by inflated metrics.	Headless-browser viewbotting tools; botting services mimicking logged-in behaviour and fake comments.
	Insurance scams	'Ghost brokers' sell fake/invalid insurance certificates; forge documents or resell/cancel real policies while keeping the victim's payment.	Reliance on organic (unpaid) social content, benefiting from algorithmic amplification without ad spend.	Generative-AI forged certificates; cloned/AI-generated insurance websites; private messaging for negotiation; impersonation of legitimate insurance brokers.

	Loan and credit offer scams	Fraudulent loan offers promise no credit checks/low rates; victim pays an upfront fee after fake 'approval', then scammer vanishes.	Manipulated search results rank fraudulent loan-comparison sites as top options; paid ads; unsolicited DMs/comments; manipulated comparison sites; weak advertiser verification.	Advance-fee mechanism; fake comparison websites; cloned lender websites.
	Rental scams	Fake/misrepresented listings collect upfront payment (vacation) or deposits (long-term); or compromised host accounts redirect guests to cloned payment.	Continuous listing feeds blending scams with legitimate rentals; trusted booking-platform messaging lends credibility once accounts are compromised; minimal listing verification.	Stolen photos/exaggerated listings; phishing/credential theft of host accounts; cloned payment pages; impersonation of hosts/landlords; off-platform payment redirection.
Employment & Collaboration Scams	**Fake job scams**	Fake recruiters offer jobs, then charge victims fees for onboarding, background checks, or admin costs.	Self-declared identity verification lets fraudsters build credible recruiter profiles; 'OpenToWork' signals target vulnerable job seekers; recruitment platform interface blending fraudulent posts with legitimate ones.	Impersonation of recruiters/companies; urgency-driven fast-hire pitches with no interviews; advance-fee requests.
	Money mule recruitment	Fake job ads recruit victims to receive/transfer illicit funds; victims are often unaware they are laundering criminal proceeds.	Same features as fake job scams; organic content (luxury-lifestyle imagery) and groups/pages on social media enable victim identification.	Social engineering promising easy compensation; migration to encrypted apps (WhatsApp/Telegram) post-recruitment.
	DM to Collab bots	Fake brand/agency sponsorship offers to content creators require upfront payment for shipping/samples; scammer vanishes after payment.	Low barriers to fake account/bot creation with minimal identity verification; private messaging functions allow reach at scale.	Automated bot networks; 'DM me' hashtags; fake 'official'/certified usernames; Brand impersonation; phishing layered onto brand impersonation
Unexpected Gain Scams	**Fake contests, raffles & prizes**	Victims are told they won a prize/contest and must pay a fee or share data to claim it.	Direct-messaging functions disseminate false winner notifications at scale.	Impersonation; advance-fee mechanism.
	Inheritance, donation & lottery scams	Unexpected message claims the victim is entitled to an inheritance, donation or lottery win, requiring an upfront fee to release funds.	Direct messaging enables mass, low-cost outreach to potential victims.	Fabricated official correspondence; advance-fee mechanism; impersonation of legal representatives, banks or other officials.
	Gambling scams	Fake casinos/betting platforms encourage small deposits, then manipulate outcomes so losses are inevitable and withdrawals are blocked.	Ad systems let unlicensed operators target users with no valid local licence; fake apps placed on legitimate app stores.	AI deepfakes of public figures; fabricated 'news' endorsements; fake gambling apps; manipulated payout mechanics; fabricated winnings displays.
	Rebate scams	False claims of entitlement to a tax/bank refund; victim pays upfront 'administrative' costs or shares personal data.	Impersonation of trusted institutions via ads/messaging with limited identity verification.	Spoofed official communications; advance-fee requests; impersonation of legal representatives, banks or other officials.
	Online penny auction scams	Users pay non-refundable per-bid fees; most participants never win the item despite repeated bidding.	Platform advertising promotes seemingly attractive low starting prices.	Paid ad placements advertising penny-auction platforms; repeated-bid fee structures designed to accumulate costs
Charity & Disaster Relief Scams	**Charity scams**	Fraudsters pose as charities during crises (disasters, conflicts) to collect donations diverted for personal gain.	Organic content distribution and recommender-system amplification of high-urgency stories; no verification of charity credentials.	Fake websites mimicking real charities; impersonation of legitimate organisations; cloned donation websites; organic social sharing for virality; co-opted trust indicators.
	Fraudulent crowdfunding campaigns	Fake fundraising campaigns (illness, disaster relief, personal projects) collect donations for causes that do not exist.	Low-friction onboarding and weak identity verification on legitimate crowdfunding platforms allow rapid fake-campaign launch.	Impersonation of charities/public figures; phishing/identity theft; emotionally manipulative imagery.

Source: *Authors' elaboration.*

Figure 1 - Scam flow diagram



Source: *Authors' elaboration.*

2.1. Investment scams

Investment scams are fraudulent schemes in which criminals promise victims significant financial returns that never materialise, stealing both the initial investment and any additional fees.[27] They operate through social media platforms, fake investment websites, and messaging applications, using tactics such as algorithmic amplification, AI-generated content, deepfake celebrity endorsements, and psychological manipulation. Investment scams are **among the most common and fast-growing types of online scams in Europe**.[28]

Investment scams are perpetrated both by lone criminals and by organised cybercrime networks.[29] These networks often **operate from jurisdictions with weak regulatory frameworks** and may involve transnational cooperation (see Section 3.2.6 for a detailed analysis of organised crime infrastructure and fraud-as-a-service models).[30]

Offenders' advertising language is deliberately deceptive, emphasising exceptionally high, immediate, and guaranteed daily returns, and framing the schemes as exclusive opportunities for fast wealth accumulation.[31] Victims of investment scams are frequently targeted again through recovery scams, in which fraudsters pose as third parties offering to help recover lost funds in exchange for upfront payments (see Section 4.3.2 for a cross-cutting analysis of re-victimisation).[32]

This typology distinguishes between traditional investment scams and cryptocurrency scams, as the latter have emerged in recent years as a trending topic and a distinct threat, involving different underlying assets. [33] The following sub-sections outline the specific characteristics of traditional investment scams and cryptocurrency-related investment scams.

---

[27] Antonis Papasavva et al., Applications of AI-Based Models for Online Fraud Detection and Analysis (2025) available at: https://link.springer.com/content/pdf/10.1186/s40163-025-00248-8.pdf.

[28] Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[29] Interpol, Interpol Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology;

[30] Waseem Nasir and Khalid Ali, Online Romance Scams and Digital Asset Fraud: Investigating Cross-Border Criminal Networks (2025) available at: https://www.researchgate.net/profile/Khalid-Ali-56/publication/389991094_Online_Romance_Scams_and_Digital_Asset_Fraud_Investigating_Cross-_Border_Criminal_Networks/links/67dbec54e62c604a0df62281/Online-Romance-Scams-and-Digital-Asset-Fraud-Investigating-Cross-Border-Criminal-Networks.pdf; Waseem Nasir, Cryptocurrency Fraud and Financial Crime: Analyzing Convicted Fraudsters in Digital Asset Scams (2025) available at: https://www.authorea.com/doi/full/10.22541/au.174180456.65670202.

[31] Debunk, Debunk.org Trusted Flagger 2025 Report (2026), available at: https://www.debunk.org/debunk-org-trusted-flagger-2025-report

[32] Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545.

[33] Interview 3.

Traditional investment scams

Traditional investment scams encompass a wide range of fraudulent schemes that promise financial returns through deceptive or misleading practices. While any type of investment can be subject to scams, several common schemes have been identified.

- **Ponzi schemes** are high-yield investment schemes that promise unusually high profits and passive income within short periods. They attract investors by offering high returns, often presented as interest payments. In practice, returns are paid using funds contributed by new investors, and the scheme collapses once the inflow of new participants declines. Participants typically believe they are investing in a legitimate financial product and are unaware they are part of a fraudulent scheme. After making their initial investment, they are usually not required to take any further action, as the scheme presents itself as a passive investment where returns supposedly come from genuine underlying assets or trading activity.[34]
- **Pyramid schemes** involve fraudsters promoting multi-level investment structures that promise exceptionally high returns with little or no risk. Participants are required to pay an entry fee and are encouraged to recruit additional members, such as friends or family. Returns are generated from the contributions of newly recruited members, which requires continuous recruitment to sustain the scheme. Unlike Ponzi schemes, participants are typically aware that their earnings depend on bringing in new members, and they must remain actively involved in recruitment. By encouraging victims to recruit other victims, fraudsters expand the network and increase their profits.[35] Those victims can also be underage.[36]
- **Penny stock scams** involve the manipulation of low-priced, thinly traded shares to artificially inflate their value, often through misleading or false promotional information. Once the price has been driven up, fraudsters sell their holdings at a profit, leaving other investors with shares that rapidly lose value. Common tactics include deceptive marketing campaigns, ‘chop stocks’ involving undisclosed commissions, and ‘dump and dilute’ schemes.[37] Although penny-stock scams are more commonly associated with North American markets, the European Securities and Markets Authority (ESMA) has warned about social-media-driven share promotion and market manipulation affecting retail investors (penny stocks are heavily driven by retail investors, i.e., non-professional

[34] Massimo Bartoletti et al., Cryptocurrency Scams: Analysis and Perspectives (2021), available at : https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9591634.

[35] Europol, Online fraud schemes – A web of deceit (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/e914d7fe-b429-11ee-b164-01aa75ed71a1/language-en.

[36] Europol, Decoding the EU's Most Threatening Criminal Networks – Issue 2: The Blueprint of Criminal Opportunism (2026) available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Blueprint-of-criminal-opportunism.pdf.

[37] DC Department of Insurance, Securities and Banking, Warning Signs of a Penny Stock Scam, available at: https://disb.dc.gov/page/warning-signs-penny-stock-scam.

individuals), particularly where online communities and influencers are used to artificially generate demand for speculative securities.[38]

- **Pre-IPO scams** involve fraudulent offers to purchase shares in a company before it becomes publicly listed. These schemes typically promise significant returns from early-stage investment in a start-up, but the opportunities are either misrepresented or entirely fictitious.[39] Although pre-IPO shares are more common in North American markets, Germany's Federal Financial Supervisory Authority (BaFin) has issued warnings regarding fraudulent offers of pre-IPO shares, noting that criminals exploit investor interest in anticipated stock market listings by offering non-existent or unauthorised securities.[40]

In terms of operationalisation, fraudsters use **paid advertisements** on social media platforms, search engines, and other digital services to promote unauthorised investment firms, cloned financial institutions, fake trading platforms, and high-yield investment opportunities. These advertisements frequently employ false celebrity endorsements, fabricated performance claims, and deepfakes.[41] Platform targeting systems enable fraudsters to reach users actively searching for investment opportunities. Regulatory authorities, such as ESMA, increasingly report that unauthorised financial promotions are disseminated through the same advertising infrastructure used by legitimate financial service providers.[42]

Migrating from online platforms towards private communication channels, scammers use private messaging group chats to simulate communities of successful investors, reducing victims' psychological resistance.[43] In these groups, artificial social proof signals are shared, including fake testimonials, fabricated profit screenshots, and coordinated discussions involving purported investment advisers.[44] In parallel, victims are redirected to fake investment

[38] ESMA, ESMA highlights risks to retail investors of social media driven share trading (2021), available at: https://www.esma.europa.eu/press-news/esma-news/esma-highlights-risks-retail-investors-social-media-driven-share-trading

[39] U.S. Securities and Exchange Commission, Risky Business: "Pre-IPO" Investing (2005), available at: https://www.sec.gov/about/reports-publications/investorpubspreipohtm.

[40] BaFin, SK Black Rock Financial GmbH: BaFin warns against unauthorised offers of pre-IPO share (2025), available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/EN/Verbrauchermitteilung/weitere/2025/meldung_2025_10_23_sk-blackrock-financial_com_en.html

[41] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”; Finans Danmark, Styrket bekæmpelse af digital svindel - Svindel Task Forcens 18 anbefalinger (2024), available at: https://www.ft.dk/samling/20241/almdel/ERU/bilag/81/2948819/index.htm.

[42] ESMA, ESMA urges social media companies to tackle unauthorised financial ads (2025), available at: https://www.esma.europa.eu/press-news/esma-news/esma-urges-social-media-companies-tackle-unauthorised-financial-ads

[43] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Anlagebetrug über WhatsApp und Telegram, available at: https://www.bafin.de/DE/verbraucherinnen-verbraucher/themen-finanzprodukte/finanzbetrug-erkennen/anlagebetrug/whatsapp-telegram/whatsapp-telegram.html; FSMA, Opgelet voor beleggingstips via WhatsApp (2026), available at: https://www.fsma.be/nl/warnings/opgelet-voor-beleggingstips-whatsapp.

[44] Jingjia Xiao, Qing Xiao and Hong Shen, “It felt real” victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

websites with fabricated dashboards displaying fictitious profits.[45] Beyond paid advertising, scammers repurpose platform features such as friend-expansion and recommendation functions to surface scam-related profiles in users' feeds.[46] AI-enabled automation tools further amplify this reach by generating high volumes of content and inflating engagement metrics.[47]

Certain characteristics inherent to online services inadvertently enable this exploitation. Recommendation algorithms prioritise engaging content, and investment narratives framed around urgency and exclusivity perform well under this logic, steering users toward fraudulent environments.[48] **Repeated algorithmic exposure can normalise implausible claims** before detection mechanisms are triggered.[49] Platform optimisation tools may further increase exposure by identifying users likely to engage with investment-related content (see Section 3.1.1 for a comprehensive analysis of platform risk factors).[50]

Cryptocurrency scams

Crypto-assets are a digital representation of value or rights that can be transferred and stored electronically using distributed ledger technology or similar systems. While some, such as stablecoins, are designed to maintain a stable value by referencing an underlying asset or official currency, many other crypto-assets derive their value primarily from market demand and investor sentiment. As a result, many crypto-assets are highly volatile and can experience substantial and rapid price fluctuations, making them high-risk investment products.[51]

---

[45] Interview 4; corroborated by Rajvardhan Oak and Zubair Shafiq, “Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf.

[46] Interviews 4, 6; corroborated by Jingjia Xiao, Qing Xiao and Hong Shen, “It felt real” victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[47] Interview 8; see also Debunk, Debunk.org Trusted Flagger 2025 Report (2026), available at: https://www.debunk.org/debunk-org-trusted-flagger-2025-report; Europol, Online fraud schemes – A web of deceit (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/e914d7fe-b429-11ee-b164-01aa75ed71a1/language-en.

[48] Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545; for a general analysis of recommender systems, see Katarzyna Szymielewicz, Reclaiming the Algorithm: What the DSA can—and can’t—fix about recommender systems (2026), available at: https://dsa-observatory.eu/2026/02/15/reclaiming-the-algorithm-what-the-dsa-can-and-cant-fix-about-recommender-systems/;

[49] Jingjia Xiao, Qing Xiao and Hong Shen, “It felt real” victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[50] ESMA, ESMA urges social media companies to tackle unauthorised financial ads (2025), available at: https://www.esma.europa.eu/press-news/esma-news/esma-urges-social-media-companies-tackle-unauthorised-financial-ads

[51] BEUC, Hype or Harm? The Great Social Media Crypto Con (2023), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-073_Hype_or_harm_The_great_social_media_crypto_con.pdf.

The diversity of crypto-assets has led to the emergence of numerous subcategories of cryptocurrency scams. Fraudsters exploit certain characteristics of blockchain technologies, particularly the possibility of exchanging crypto assets anonymously or pseudonymously for fiat currencies.[52]

- **Fake Initial Coin Offerings (ICOs)** involve fraudulent fundraising schemes that imitate legitimate token launches to lure investors into purchasing worthless or non-existent coins.[53] Fraudsters replicate the ICO model, which resembles an initial public offering, to raise funds. In some cases, so-called 'scam coins' are deployed through malicious smart contracts that allow unauthorised access to users' wallets. These contracts may include hidden functions, such as excessive transaction fees or pre-approved transfers, enabling developers to extract funds at any time.[54] According to Dowlat and Hodapp, 80% of all ICOs launched in 2017 were estimated to be scams.[55]
- **Non-fungible Token (NFT) scams** involve fraudulent schemes linked to NFTs, which are cryptographic digital assets, such as a JPG image, memes, sports cards, video, music, or digital artwork, recorded on a blockchain with unique identifiers. In these scams, fraudsters may promote NFT projects that appear legitimate to attract investment.[56] One common form is the 'rug pull', where an NFT project is heavily promoted to generate interest and sales and then abruptly abandoned by its scammers.[57] As a result, investors (i.e. victims) are left unable to recover their assets. These scams may take the form of technical manipulation, such as altering smart contracts to prevent sales or impose excessive fees, or promotional 'exit scams', where a token is heavily marketed before the organisers withdraw funds.[58] They may also involve the creation of fake websites and the impersonation of customer support, wherein fraudsters may steal personal data from the victim.[59]

---

[52] Massimo Bartoletti et al., Cryptocurrency Scams: Analysis and Perspectives (2021), available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9591634.

[53] ibid; Vasilka Chergarova et al., Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest into cryptocurrency (2022), available at: https://iacis.org/iis/2022/3_iis_2022_242-252.pdf.

[54] Vasilka Chergarova et al., Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest into cryptocurrency (2022), available at: https://iacis.org/iis/2022/3_iis_2022_242-252.pdf.

[55] Sherwin Dowlat and Michael Hodapp, Cryptoasset Market Coverage Initiation: Network Creation (2018), available at: https://research.bloomberg.com/pub/res/d28giW28tf6G7T_Wr77aU0gDgFQ.

[56] Fraud.com, NFT Scams – Real-life story, available at: https://www.fraud.com/post/nft-scams-a-real-life-story#:~:text=Fake%20Websites:%20Fake%20trading%20sites,are%20stolen%20by%20the%20creators

[57] Interpol, Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf.

[58] Solidus Labs, What is a Rug Pull? DeFi Scams Explained (2022), available at: https://www.soliduslabs.com/post/rug-pull-crypto-scams.

[59] Fraud.com, NFT Scams – Real-life story, available at: https://www.fraud.com/post/nft-scams-a-real-life-story#:~:text=Fake%20Websites:%20Fake%20trading%20sites,are%20stolen%20by%20the%20creators

- **Fake exchange scams** deceive users by offering highly favourable conditions for purchasing cryptocurrencies. These platforms promote easy access to low-cost digital assets but are fraudulent, and funds deposited by users are misappropriated.[60]
- **Fake wallet scams** exploit cryptocurrency wallet services. Fraudulent providers imitate legitimate wallets used to store and transfer crypto-assets but ultimately gain access to users' credentials or private keys and steal their funds.[61]
- **Airdrop scams** exploit the appeal of free cryptocurrency distributions to deceive users. Legitimate airdrops are marketing initiatives in which blockchain projects provide tokens to users to increase awareness or reward participation. Scammers create fake airdrop campaigns and distribute worthless tokens to random wallet addresses. When recipients attempt to trade or transfer these tokens, the transaction fails and generates an error message, which then directs victims to a fake website or fraudulent platforms. Users are then prompted to connect their digital wallets to claim or exchange the tokens. By doing so and approving requested transactions, victims may unknowingly authorise malicious smart contracts. These contracts enable unauthorised transfers of assets, resulting in the rapid loss of legitimate cryptocurrency holdings from the victim's wallet.[62]
- **Fake mining pool scams** target cryptocurrencies based on proof-of-work mechanisms. Victims are encouraged to invest in mining hardware or join mining pools with promises of returns. In reality, funds are not used for mining activities but redistributed to earlier participants, often resembling a Ponzi structure.[63]
- **Fake mixing scams** exploit the traceability of transactions on blockchain systems such as Bitcoin. Since transactions are publicly recorded and linked together, it is possible to trace the movement of cryptocurrency between addresses. Mixing services are designed to obscure these links by randomising transactions, introducing delays, and routing funds through multiple intermediary addresses. In fraudulent cases, fake mixing services receive cryptocurrency from users but simply steal the funds without performing the promised mixing service.[64]
- **Cryptocurrency giveaway scams** set up fake websites that abuse the names and images of celebrities to advertise 'giveaway' events, purportedly to popularise cryptocurrencies. These sites promise to double or triple the funds that users send to a specific wallet address, which is in fact controlled by the scammer who then drives traffic to these websites through any means possible, most commonly by compromising popular YouTube channels and social-media accounts.[65] The victim is requested to send a specific

[60] Massimo Bartoletti et al., Cryptocurrency Scams: Analysis and Perspectives (2021), available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9591634.

[61] ibid.

[62] Ledger Adademy, Airdrop Scams (2025), available at: https://www.ledger.com/academy/glossary/airdrop-scams

[63] ibid.

[64] ibid.

[65] Vilma Luoma-aho et al., Vulnerabilities to Crypto Currency Scams and Online Persuasion Strategies (2025), available at: https://jyx.jyu.fi/bitstreams/5459bc01-0ded-457b-b4ab-45617cbecc08/download; Xigao Li et al.,

amount of crypto to a given crypto address, with the promise that the platform would give away double the amount sent by the investor.[66] The logic and arguments the scammers use to get the victim to send bitcoins are that the platform can verify the wallet address and the legitimacy of the investor's account. Social media sites are often used to market or announce giveaway scams. These scams frequently involve the impersonation of well-known individuals, companies or influencers on social media platforms, and may use manipulated livestreams or direct messages to create a sense of legitimacy.[67] Liu et al. measured how cryptocurrency giveaway scams operate on X, YouTube and Twitch. They found that victimisation rates varied across platforms, ranging from approximately 4 victims per 100,000 livestream views on some platforms to around 1 victim per 1,000 views on others. Based on these estimates, the authors concluded that scammers extracted nearly USD 4.62 million (EUR 4 million) from several hundred victims between January and June 2022.[68]

- **Crypto-based Ponzi schemes** use cryptocurrency as the payment mechanism within a traditional Ponzi structure. Participants are provided with online accounts displaying apparent profits and are encouraged to recruit new members. Returns are presented as being generated through activities such as cloud mining, automated trading, or lending, but are in fact financed by new investors. These schemes collapse once new recruitment declines, with later participants incurring the greatest losses.[69]
- **Crypto-based pump-and-dump scams** artificially inflate the price of a crypto-asset to profit from its subsequent collapse. The scheme typically begins with coordinated promotion designed to generate hype and attract investors. Organisers may use messaging platforms or online communities to announce a planned 'pump' and encourage participants to buy a particular low-value token at a specified time. The identity of the token is often revealed only shortly before the event. As large numbers of investors place buy orders, the price rapidly increases. However, the organisers and early participants usually purchase the asset in advance and sell their holdings once the price rises. This large-scale selling triggers a sharp price decline, leaving late investors with significant losses. In some cases, organisers promise a second wave of price increases to maintain interest and encourage further purchases. In reality, the additional price surge rarely occurs.[70]

Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams (2023), available at: https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_f584_paper.pdf.

[66] European Banking Authority, Fraudes et Escroqueries Liées aux Crypto-Actifs : Restez Vigilant(E) et Protégez-Vous, available at: https://www.cssf.lu/wp-content/uploads/Fraudes-et-escroqueries-liees-aux-crypto-actifs.pdf.

[67] ibid; Vilma Luoma-aho et al., Vulnerabilities to Crypto Currency Scams and Online Persuasion Strategies (2025), available at: https://jyx.jyu.fi/bitstreams/5459bc01-0ded-457b-b4ab-45617cbecc08/download; Xigao Li et al., Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams (2023), available at: https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_f584_paper.pdf.

[68] Enze Liu et al., Give and Take: An End-To-End Investigation of Giveaway Scam Conversion Rates (2024), available at: https://arxiv.org/pdf/2405.09757.

[69] Vilma Luoma-aho et al., Vulnerabilities to Crypto Currency Scams and Online Persuasion Strategies (2025), available at: https://jyx.jyu.fi/bitstreams/5459bc01-0ded-457b-b4ab-45617cbecc08/download.

[70] Ibid; Massimo Bartoletti et al., Cryptocurrency Scams: Analysis and Perspectives (2021), available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9591634.

- **Fake memecoins** also constitute a form of cryptocurrency scams. Memecoins are virtual coins that typically originate from internet 'memes', such as humorous or satirical images, videos, or text shared on social media platforms. Unlike more established crypto-assets with identifiable utility or governance structures, many memecoins are purely speculative and derive their value largely from online attention, social media promotion, and celebrity endorsement. While memecoins are traded on various crypto platforms, they are often heavily promoted by finfluencers on social media platforms, who may use their reach to artificially increase demand and inflate prices. Due to their high volatility, the value of memecoins depends almost entirely on market attention and investor sentiment. As a result, finfluencers can significantly affect the market value of memecoins by promoting, criticising, or ignoring particular tokens. However, the information shared by finfluencers may be unreliable, as many lack sufficient financial expertise or may have undisclosed financial interests in the promoted assets[71].

While the same type of offenders of traditional investment scams also perpetrate cryptocurrency scams, recent events suggest that offenders are also located in Western Europe – for example, Belgian and Swiss law enforcement authorities dismantled a criminal network running a worldwide Ponzi scheme using pyramid selling of the cryptocurrency 'VITAE'. [72] The members of this criminal network were found to be mostly Belgian nationals who were making use of a company under Swiss jurisdiction.[73]

Social media platforms can function as core advertising and recruitment infrastructure for cryptocurrency scams, valued by fraudsters for the wide reach of their ad placement services (see Section 3.1.1 for a comprehensive analysis of platform risk factors).[74] Fake advertisements are used to redirect users toward spoofed websites, fraudulent trading platforms, or fake cryptocurrency wallets. These ads frequently promise highly unrealistic returns and combine exaggerated profit projections with psychologically manipulative marketing techniques, including narratives around passive income, 'AI trading bots', and 'advanced staking plans'.[75] Cryptocurrency scams are also promoted on social media platforms, particularly video-sharing platforms, by 'finfluencers' – this dynamic is further explored in case study A (Section 6.1.).

---

[71] BaFin, Memecoins: Glücksspiel statt Geldanlage (n.d.), available at: https://www.bafin.de/DE/verbraucherinnen-verbraucher/themen-finanzprodukte/finanzbetrug-erkennen/anlagebetrug/memecoins/memecoins_node.html

[72] Europol, Europol Spotlight - Cryptocurrencies: tracing the evolution of criminal finances (2022), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

[73] ibid.

[74] Gen, Gen Q4/2024 Threat Report (2024), available at: https://www.gendigital.com/blog/insights/reports/threat-report-q4-2024; Interpol, Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf; Competition and Consumer Protection Commission (CPCC), Scams – Real cases, real consequences: A collection of case studies and lessons for consumers (2025), available at: https://www.ccpc.ie/consumers/wp-content/uploads/sites/2/2025/11/Scams-Real-cases-real-consequences-CCPC.pdf; Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545.

[75] Debunk, Debunk.org Trusted Flagger 2025 Report (2026), available at: https://www.debunk.org/debunk-org-trusted-flagger-2025-report.

Similar to traditional investment scams, private messaging applications, are exploited to create fraudulent communities promoting fake investment opportunities.[76] Victims are subjected to persistent solicitation and artificial time pressure. Deepfake technology and AI-generated content are increasingly deployed to impersonate trusted individuals, reinforcing the appearance of legitimacy.[77]

Platform features designed for engagement and reach are **structurally advantageous to fraudsters**. The wide reach of programmatic ad placements on major platforms enables fraudulent cryptocurrency advertisements to reach large audiences rapidly, exploiting the same targeting infrastructure available to legitimate advertisers.[78] Crucially, **cryptocurrency content is frequently marketed on social media in ways that expose users with low financial literacy to manipulative investment narratives** before they have developed the capacity to critically evaluate them. Research supports this concern; studies find that social media algorithms can inundate users who display even basic curiosity in cryptocurrency with content that promotes and exaggerates profitability, initially appearing informational before transitioning to manipulation that exploits the fear of missed opportunity and overconfidence.[79] Once initial contact is established on a platform, victims are redirected to external fraudulent infrastructure, meaning designated services function as the entry point of a broader scam ecosystem that extends beyond their direct environment.

2.2. Romance scams

Romance scams are fraudulent schemes in which criminals construct fictitious romantic relationships with victims, typically through social media platforms or messaging services, with the deliberate intention of exploiting the emotional trust and dependency that develops to extract money, personal information, or other financial value from the victim. This section distinguishes between traditional romance scams, romance baiting and sextortion, with the latter two identified as specific, hybridised configurations of the former.

Traditional romance scams

Traditional romance scams refer to a form of online scam in which offenders create the appearance of a genuine emotional or romantic relationship in order to obtain financial gain. These relationships are typically established online and are maintained over time to build trust.

[76] BaFin, Investitionen in Kryptowerte und der Einfluss sozialer Medien auf das Anlageverhalten (2026), available at: https://www.bafin.de/DE/Aufsicht/Fokusrisiken/Fokusrisiken_2026/RIF_verbraucher_sozialemedien/RIF_verbraucher_sozialemedien_node.html;jsessionid=7482B626CD4BA5A50D21116827D3E0A2.internet012.

[77] Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/; Gendigital, Gen Q3/2025 Threat Report (2025), available at: https://www.gendigital.com/blog/insights/reports/threat-report-q3-2025.

[78] Debunk, Debunk.org Trusted Flagger 2025 Report (2026), available at: https://www.debunk.org/debunk-org-trusted-flagger-2025-report; Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[79] Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545.

Victims are persuaded to voluntarily transfer money through electronic means, often under the belief that they are assisting a partner in need.[80] Unlike other emotionally driven scams, such as friendship scams or family impersonation scams, romance scams specifically exploit the victim's perception of an intimate or romantic relationship.[81] Stakeholders interviewed for this study highlighted the importance of timing in romance scam campaigns, noting that fraudsters often intensify their activities around Valentine's Day, when individuals may be more receptive to online relationship-building and emotional manipulation.[82]

In recent years, corporate entities have also emerged that market themselves to potential employees and clients as social media or customer service management companies, but which in practice operate as commercialised romance fraud businesses. These firms recruit individuals online as 'chat moderators' or 'customer service providers', claiming they will use customer service databases to handle client complaints or service requests, or to support engagement on new social media platforms. In practice, however, workers are often recruited for paid 'sexting' roles, where they are paid per message (typically around 1–2 euros) to engage in sex chat with clients who believe they are interacting with genuine users. Workers are provided with background information on clients, including photos and personal histories, and are instructed to present themselves as potential romantic or intimate partners. The entire process is mediated by algorithmic systems that monitor productivity and monetise interactions between workers and clients. This model simultaneously victimises clients, who are deceived into paying for fictitious intimate relationships, and workers, who are often unaware of the deceptive nature of the work and may also experience wage theft.[83] It should be noted that this business model raises separate labour-exploitation concerns, as the recruited workers are frequently unaware of the deceptive nature of the role for which they were hired and may themselves experience wage theft. These worker-related harms fall outside the scope of the fraud-victim definition adopted in this report.

The execution of a romance scam begins with the scammer creating an attractive profile on a dating site or social media platform that replicates a celebrity or figure of authority or portrays an entirely fictitious identity. Once the profile has been created, the scammer reaches out to potential victims and lures them into an online conversation. After communication has been established, the grooming phase follows, whereby the scammer seeks to establish a strong, well-trusted, emotional relationship before the victim is asked for financial support to overcome a tragic or desperate situation. Reasons for the monetary requests may include inheritance fees, plane tickets, visa fees, family emergencies, or presents. While some scams last only a few days, most span several months, and some continue for years; in extreme cases, up to 8 years, either when the victim runs out of money or realises they have been targeted.[84] Though victims of romance scams directly provide their fraudster with financial support, they may also

[80] Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670; Cassandra Cross and Karen Holt, To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581.

[81] Multi-stakeholder Workshop on Online Financial Scams.

[82] Multi-stakeholder Workshop on Online Financial Scams.

[83] Fangzhou Wang and Volkan Topalli, The Cyber-Industrialization of Catfishing and Romance Fraud (2023), available at: https://www.sciencedirect.com/science/article/pii/S0747563223004843?via%3Dihub

[84] Schokkenbroek & Snaphaan, Love as Bait: A Scoping Review and Crime Script Analysis of Online Romance Scams (2025), available at: https://journals.sagepub.com/doi/full/10.1177/15248380251361046; Alexander Bilz et al., Tainted Love: a Systematic Literature Review of Online Romance Scam Research (2023), available at: https://academic.oup.com/iwc/article/35/6/773/7331428.

give out sensitive personal information, such as bank account details, as a part of their communication with an offender.[85]

After the scam has been conducted, victims are especially prone to re-victimisation, as they are in a vulnerable psychological state following prolonged manipulation (see Section 4.3.2 for further analysis). Strategies include the scammer admitting the scam but claiming to have developed genuine feelings for the victim, recovery scams in which a third party offers to help recover lost money,[86] and the sharing of victim information via 'sucker lists'.[87]

Victims are approached via cold call messages expressing intentions of a deeper conversation, asking users to move to a different communication channel.[88] This migration to private channels is designed to bypass moderation and reporting mechanisms.[89] Financial requests are subsequently introduced through advance-fee mechanisms framed around urgency and fabricated personal crises.

Despite common assumptions that men predominantly perpetrate online romance scams, recent literature reports that women also play active roles as perpetrators.[90] One reason is that women seek direct and profitable online contacts without relying on men for mentorship and support.[91] Scammers can thus be male or female; however, the fake profile scammers use depends on the victim. Female profiles, portraying themselves as no older than 30 years and working in low-paying or non-professional jobs, such as a nurse, student, or teaching assistant, tend to target heterosexual male victims in their later years and include a photo of a conventionally beautiful woman, often with no children.[92] For profiles targeting heterosexual females, the profiles typically claimed to be as old as 50 but mostly younger than the victim.[93] Occupations include professional jobs, entrepreneurial activities, or army ranks. For fake male

[85] Cassandra Cross and Karen Holt, To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581.

[86] Monica Whitty, The online dating romance scam: The psychological impact on victims–both financial and non-financial (2015), available at: https://journals.sagepub.com/doi/abs/10.1177/1748895815603773.

[87] Schokkenbroek & Snaphaan, Love as Bait: A Scoping Review and Crime Script Analysis of Online Romance Scams (2025), available at: https://journals.sagepub.com/doi/full/10.1177/15248380251361046

[88] Tenable, Pig Butchering Scam: From Tinder and TikTok to WhatsApp and Telegram, How Scammers Are Stealing Millions in a Long Con (2024), available at: https://www.tenable.com/blog/pig-butchering-scam-tinder-tiktok-whatsapp-telegram-scammers-steal-millions#contactingvictims.

[89] Janneke M Schokkenbroek and Thom Snaghaan, Love as Bait: A Scoping Review and Crime Script Analysis of Online Romance Scams (2025), available at: https://journals.sagepub.com/doi/10.1177/15248380251361046.

[90] Lazarus et al. What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021) (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000131.

[91] ibid.

[92] Rasha Kassem and Elisabeth Carter, Mapping romance fraud research – a systematic review (2024), available at: https://www.emerald.com/jfc/article-abstract/31/4/974/1238258/Mapping-romance-fraud-research-a-systematic-review?redirectedFrom=fulltext; Monica Whitty, Do You Love Me? Psychological Characteristics of Romance Scam Victims (2018), available at: https://journals.sagepub.com/doi/full/10.1089/cyber.2016.0729.

[93] ibid.

homosexual profiles, age ranges are generally younger than 30 years and claim mixed professional status.[94]

Offenders involved in traditional romance scams operate both individually and within organised structures. **Socio-economic drivers such as poverty, unemployment and limited income opportunities** have been identified as contributing factors to offending, alongside peer recruitment mechanisms.[95] Perpetrators typically possess a certain level of digital literacy, including the use of tools such as virtual private networks (VPN). Offender activity has frequently been linked to **regions such as West Africa and the Philippines**.[96] Overall, organised cybercrime networks are often based in **jurisdictions with limited regulatory enforcement**, enabling such activities to be conducted with reduced risk of prosecution.[97] These networks may involve hierarchical structures with clearly defined roles, as observed in some West African organised crime groups. There is also evidence of **transnational cooperation**, including links with organised crime groups in the Middle East and Europe, as well as operational centres believed to be located in Eastern Europe and parts of Africa.[98] Despite this, a significant proportion of traditional romance scams continues to be conducted by individuals or loosely organised groups; in that sense, an interviewee claimed it has become **very accessible to create fake online profiles and solicit money from victims**.[99]

Social media platforms, messaging applications and dating platforms are structurally embedded in how these scams are initiated, sustained, and ultimately used to extract financial value from victims.[100] Platform design features, including low barriers to account creation, algorithmic recommendation systems, persistent messaging, and contact synchronisation, can create conditions that scammers exploit throughout the scam lifecycle (see Section 3.1.1 for a comprehensive analysis of platform risk factors).[101] Once emotional trust is established

[94] Lazarus et al. What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021) (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000131.

[95] Alexander Bilz et al., Tainted Love: a Systematic Literature Review of Online Romance Scam Research (2023), available at: https://academic.oup.com/iwc/article/35/6/773/7331428.

[96] Matthew Edwards, Online sextortion: Characteristics of offences from a decade of community reporting (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000386.

[97] Waseem Nasir and Khalid Ali, Online Romance Scams and Digital Asset Fraud: Investigating Cross-Border Criminal Networks (2025) available at: https://www.researchgate.net/profile/Khalid-Ali-56/publication/389991094_Online_Romance_Scams_and_Digital_Asset_Fraud_Investigating_Cross-_Border_Criminal_Networks/links/67dbec54e62c604a0df62281/Online-Romance-Scams-and-Digital-Asset-Fraud-Investigating-Cross-Border-Criminal-Networks.pdf.

[98] Interpol, Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf.

[99] Interview 1.

[100] Matthew Edwards, Online sextortion: Characteristics of offences from a decade of community reporting (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000386.

[101] Amy Lim and Kyung-shick Choi, Modus operandi and blockchain analysis of romance scams: Cryptocurrency-driven victimization (2025), available at: https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1220&context=ijcic; Jingjia Xiao, Qing Xiao and Hong

within the platform environment, victims are transitioned to private messaging channels outside platform oversight.

Data from 2025 published by the US Federal Trade Commission (US FTC) confirms the centrality of platforms to this specific scam type: **nearly 60% of people who reported losing money to a romance scam said it started on a social media platform**, with Facebook being the most frequently identified platform, followed by WhatsApp and Instagram.[102]

Romance baiting

Recent years have seen a convergence between romance scams and investment scams, giving rise to a novel hybrid scam model, namely romance baiting (variations of which are also referred to as 'cryptorom' or 'pig butchering', the latter originating from its first appearance in China in the early 2010s).[103] Despite the difference in terms, they all 'largely refer to the same process'.[104] These approaches combine elements of **emotional manipulation with fraudulent investment opportunities**, most commonly involving cryptocurrencies.

Romance baiting is still classified under romance scams because the initial and central mechanism of deception relies on the deliberate construction of an intimate relationship. Offenders establish what appears to be a genuine personal relationship with the victim and subsequently introduce an investment opportunity, often framed as a trusted recommendation based on personal or family experience.[105] Romance baiting scams differ from traditional romance and investment scams by combining **prolonged emotional manipulation with sophisticated fraudulent investment schemes**. Romance-baiting scammers **invest months building trust and relationships**.[106]

Romance baiting is predominantly operated by organised cybercrime networks, often based in jurisdictions with weak regulatory enforcement, which enables them to operate at scale with limited risk of prosecution.[107]

Romance baiting combines the **platform affordances and operational tools characteristic of both romance scams and investment scams**. The platform features that enable this

Shen, "It felt real" victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[102] US Federal Trade Commission, Reported losses to scams on social media eight times higher than in 2020 (2026), available at: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2026/04/reported-losses-scams-social-media-eight-times-higher-2020#ft5.

[103] Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670.

[104] ibid.

[105] ibid.

[106] Rajvardhan Oak and Zubair Shafiq, "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf.

[107] Waseem Nasir and Khalid Ali, Online Romance Scams and Digital Asset Fraud: Investigating Cross-Border Criminal Networks (2025), available at: https://www.researchgate.net/profile/Khalid-Ali-56/publication/389991094_Online_Romance_Scams_and_Digital_Asset_Fraud_Investigating_Cross-_Border_Criminal_Networks/links/67dbec54e62c604a0df62281/Online-Romance-Scams-and-Digital-Asset-Fraud-Investigating-Cross-Border-Criminal-Networks.pdf.

hybrid scam type include social media environments that facilitate initial contact and relationship-building; low barriers to account creation and limited identity verification that enable the construction of false personas; algorithmic recommendation systems that surface potential victims; and private messaging functionalities that allow migration to channels beyond platform oversight.[108] The relevant platform risk factors, tools, and behavioural models are described in the sections above on investment scams and on traditional romance scams, as well as in Section 3.1.1 below. Moreover, the misuse of social media platforms for romance baiting is further explored in case study B (Section 6.2.).

Sextortion

Sextortion is a form of romance scam that differs from traditional romance scams or romance baiting as it centres on **coercion and blackmail** involving explicit material, rather than the development of a sustained romantic relationship. It typically involves offenders **claiming to possess, obtain or create intimate images or videos** of a victim and using this material to extort money. While distinct, sextortion may also emerge from traditional romance scams that evolve into coercive situations. In some cases, offenders further exploit victims by posing as authorities or recovery agents offering assistance, which constitutes an **additional layer of scamming**.[109]

At least three main forms can be distinguished. Under the first, offenders threaten to disclose existing explicit content unless payment is made, whilst, under the second, victims are manipulated or coerced into producing such material under threats of exposure or harm.[110] Under the third, offenders use generative AI to manipulate ordinary, non-explicit images or videos of a victim, such as photos already shared on social media, into fabricated sexually explicit material, which is then used as the basis for extortion or which itself constitutes newly created abuse material.[111]

While sextortion is a crime that can target anyone of any age, law enforcement agencies and helplines have identified **young people aged 15 to 17** and **adults aged 18 to 30** as being at greater risk.[112] The Revenge Porn Helpline, based in the UK and dealing with cases of intimate image abuse, found that sextortion was the most reported type of issue to the helpline in 2022.[113] Their annual report also suggests that the number of men contacting the helpline has

[108] Amy Lim and Kyung-shick Choi, Modus operandi and blockchain analysis of romance scams: Cryptocurrency-driven victimization (2025), available at: https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1220&context=ijcic.

[109] Jacqueline M Drew and Julianne Webster, The victimology of online fraud: A focus on romance fraud victimisation (2024), available at: https://www.sciencedirect.com/science/article/pii/S2949791424000058.

[110] Cassandra Cross and Karen Holt, To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581.

[111] National Center for Missing & Exploited Children, Generative AI (GAI), available at: https://www.missingkids.org/theissues/generative-ai.

[112] European Union, Better Internet for Kids – Sextortion, available at: https://better-internet-for-kids.europa.eu/en/learning-corner/teachers-and-educators/sextortion.

[113] SWGfL, Revenge Porn Helpline 2022 Annual Report (2022), available at: https://swgfl.org.uk/research/revenge-porn-helpline-2022-report/.

risen each year, suggesting that men are increasingly targeted by this crime.[114] This echoes the experiences of the WeProtect Global Alliance, which has found that boys and men are targeted by sextortion more frequently than women and girls, justifying that boys are more likely to be lax with the use of passwords, often communicate with strangers online and appear to be more confident than girls in their ability to distinguish the real from the fake online.[115] Statistics from the U.S. in 2022 report that law enforcement agencies received over 7000 reports of online sextortion against over 3000 victims in the USA, predominantly boys.[116] Further data from the U.S. finds that 90% of victims of financial sextortion were males aged between 14 and 17.[117]

Sextortion is carried out both by individuals and organised actors. Offenders may include cybercriminals who obtain compromising material through hacking or deception, former or current intimate partners, and transnational organised crime groups operating at scale.[118] These networks are often based in regions with limited regulatory enforcement, enabling them to operate with reduced risk of prosecution.[119] Reported offender profiles frequently indicate links to regions such as West Africa, the Philippines and the Middle East.[120] In many cases, offenders adopt false identities, often presenting themselves as young women to establish initial contact and increase engagement.[121] While this behaviour is largely committed by organised criminal gangs, there is also the potential for young people themselves to be drawn into committing this type of offence against others. In 2022, the University of East London found that 1 in 13 European youth aged 16 to 19 had engaged in sextortion online.[122]

[114] ibid.

[115] WeProtect Global Alliance, A web of deceit: financial sexual extortion of children and young people (2024), available at: https://www.weprotect.org/resources/library/financial-sexual-extortion-of-children-and-young-people/.

[116] FBI, International Law Enforcement Agencies Issue Joint Warning about Global Financial Sextortion Crisis (2023), available at: https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis.

[117] Thorn, Trends in Financal Sextortion – An investigation of sextortion reports in NCMEC CyberTipline data (2024), available at: https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf.

[118] Matthew Edwards, Online sextortion: Characteristics of offences from a decade of community reporting (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000386.

[119] Waseem Nasir and Khalid Ali, Online Romance Scams and Digital Asset Fraud: Investigating Cross-Border Criminal Networks (2025) available at: https://www.researchgate.net/profile/Khalid-Ali-56/publication/389991094_Online_Romance_Scams_and_Digital_Asset_Fraud_Investigating_Cross-_Border_Criminal_Networks/links/67dbec54e62c604a0df62281/Online-Romance-Scams-and-Digital-Asset-Fraud-Investigating-Cross-Border-Criminal-Networks.pdf.

[120] Matthew Edwards, Online sextortion: Characteristics of offences from a decade of community reporting (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000386; Interpol, Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf.

[121] Matthew Edwards, Online sextortion: Characteristics of offences from a decade of community reporting (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000386.

[122] European Union, Better Internet for Kids – Sextortion (n.d.), available at: https://better-internet-for-kids.europa.eu/en/learning-corner/teachers-and-educators/sextortion.

Sextortion draws on the **same platform affordances and operational tools identified in the romance scams** section above. Key enabling platform features include social media platforms that facilitate initial contact with potential victims; profile discovery and recommendation systems that enable targeted approaches; direct messaging functionalities that allow private communication and the solicitation of intimate material; and the ease of creating fake accounts and fake images that enable offenders to adopt false identities. These factors are further addressed in Section 3.1.1 below.

2.3. E-commerce scams

E-commerce scams are fraudulent schemes relying on the exchange of goods or services; scammers attract victims through low prices, miraculous claims, or exclusive access. While the victims often believe they are engaging in legitimate commercial relations and provide payment for the expected goods or services, they often do not receive the expected product or receive a very low-quality version. Respondents to the survey indicated that e-commerce scams are among the most common types of online scams in Europe, alongside investment scams.[123] They are primarily disseminated through social media platforms, search engines and online marketplaces.[124] A main risk factor on online platforms in relation to e-commerce scams is their advertising system, which is discussed in detail under Section 3.1.1. The following paragraphs describe different types of scams related to e-commerce.

Undelivered products or services

Undelivered product and service scams, otherwise referred to as fake webshops or ghost stores, involve fraudsters operating fraudulent online storefronts that advertise products or services, typically at implausibly low prices, collect advance payments, and then either disappear entirely or fail to fulfil the contract. In this scenario, victims receive nothing; the alternative, whereby victims receive cheap counterfeits in place of the advertised product, is discussed in the section below.

The psychological mechanisms exploited by scammers (**implausibly low prices combined with urgency signals** such as countdown timers, limited stock warnings, and discounts of up to 80%) are well-suited to the **fast-scrolling, high-stimulus environment of social media feeds, where critical evaluation is structurally suppressed**.[125] Survey respondents indicate that scammers **concentrate their activity around periods of peak consumer spending**: Black Friday, the pre-Christmas period, and the post-Christmas returns season; they exploit the elevated volume and speed of online purchasing behaviour at precisely the moments when platform advertising activity is also at its highest.[126] In this sense, the

[123] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[124] ibid.

[125] Competition and Consumer Protection Commission (CCPC), *Scams – Real cases, real consequences* (2025), available at: https://www.ccpc.ie/consumers/wp-content/uploads/sites/2/2025/11/Scams-Real-cases-real-consequences-CCPC.pdf.

[126] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

commercial rhythms of online platforms create predictable windows of heightened vulnerability that are systematically exploited.

Once victims are directed to a fake storefront, two operational methods are employed. One is straightforward fraudulent selling, in which payment is collected for goods that are never dispatched, with the payment typically processed through payment platforms or credit card processors that offer limited consumer recourse.[127] The second is **credit card harvesting**, whereby a spoofed payment interface collects victims' card and contact data before forwarding them to a functioning payment gateway, leaving their credentials available for further criminal exploitation.[128] Non-delivery scams are often perpetrated by criminal networks operating under an **'infrastructure-as-a-service' model**, in which a core team manages technical infrastructure while a decentralised network operates fraudulent shops.[129] This model is discussed in more detail in Section 3.2.6.

Online platforms, particularly social media and marketplaces, and online search engines serve as the primary discovery and distribution infrastructure through which non-delivery scams reach victims, with platform advertising systems and algorithmic visibility mechanisms playing a central enabling role, as explained below.

Fraudsters reach victims through two principal platform-based channels: paid advertising on social media platforms and search engines and manipulated search engine results designed to surface fraudulent storefronts organically.[130] In that sense, vzbv reports that the five most wide-reaching fake webshops it identified generated 134 million ad impressions on Google's designated services.[131] Similarly, an investigation by ÖIAT identified 36,725 fraudulent ads promoting fake webshops on Facebook between January and April 2025, reaching approximately 85.9 million users in the EU.[132] ÖIAT's report claims that Facebook did not remove or block any of the identified fake webshop pages reported by ÖIAT as a trusted flagger between the end of April and mid-May 2025.[133] These main channels are primarily discussed under Sections 3.1.1. and 3.2.1. Moreover, the advertisement of fake webshops on search engines is also explored in case study D (Section 6.4.).

[127] ECC-Net, Fraud in Cross-border E-commerce (2016), available at: https://www.eccnet.eu/publication/online-fraud; Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar.

[128] Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar.

[129] Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar.

[130] Verbraucherzentrale Bundesverband, Jeder zweite Fakeshop schaltet Werbung auf Google oder Meta (2025), available at: https://www.vzbv.de/pressemitteilungen/jeder-zweite-fakeshop-schaltet-werbung-auf-google-oder-meta; Numerous fraudulent ghost stores on Facebook and Instagram (2025), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Ghost_Stores_Erhebung_en.pdf; Makoto Shimamura, Uncovering Black-hat SEO based fake E-commerce scam groups from their redirectors and websites (2025), available at: https://arxiv.org/html/2505.21021v1

[131] ibid.

[132] Numerous fraudulent ghost stores on Facebook and Instagram (2025), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Ghost_Stores_Erhebung_en.pdf.

[133] ibid.

Beyond paid placements, survey respondents report that fake webshops are promoted through organic content on social media and through hidden links embedded in online marketplaces, where victims are redirected to external fraudulent webshops under the pretence of better offers.[134] These fake websites are further described under Section 3.2.3.

Platform design features and commercial logics may create conditions that are structurally advantageous to non-delivery fraudsters. Interviewees and survey respondents indicate that paid advertising systems on social media platforms and search engines apply the same automated placement mechanisms to fraudulent campaigns as to legitimate ones, with limited capacity to distinguish between the two at the point of distribution; this aspect is detailed in Section 3.1.1.[135] Survey respondents also indicate that algorithmic recommendation and search ranking systems can surface fraudulent storefronts organically, without any paid promotion; this phenomenon is also further described in Section 3.1.1.[136]

Counterfeit products

This type of scam involves the sale of **counterfeit versions of popular or well-known products** through online channels, typically at unusually low prices. To appear legitimate, fraudsters often present their webshops as outlet stores, exploiting consumers' familiarity with the brand name. It is worth noting that online markets for counterfeits encompass both situations in which **consumers are deceived, and those in which they willingly seek to purchase fake goods**.[137] In so-called 'primary markets', users are misled to believe that counterfeit products are genuine, for example through deceptive listings on e-commerce platforms. However, by contrast, in 'secondary markets', consumers are presumed to be sufficiently informed about the fraudulent nature of the product, through signals such as unusually low prices or explicit mention that the product is a replica.[138] This **dual nature complicates the interpretation of data** regarding trade in counterfeits, as a clear distinction between the two situations is not always present.

[134] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[135] Interviews 4, 5; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA"; see also Verbraucherzentrale Bundesverband, Jeder zweite Fakeshop schaltet Werbung auf Google oder Meta (2025), available at: https://www.vzbv.de/pressemitteilungen/jeder-zweite-fakeshop-schaltet-werbung-auf-google-oder-meta; Gen, The Scam Ad Machine (2026), available at: https://www.gendigital.com/blog/insights/research/scam-ad-machine-meta.

[136] Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[137] OECD/EUIPO, Misuse of E-Commerce for Trade in Counterfeits (2021), available at: https://www.oecd.org/en/publications/misuse-of-e-commerce-for-trade-in-counterfeits_1c04a64e-en.html

[138] ibid.

To evade automated counterfeit-detection systems, fraudsters deliberately use terms such as 'dupe' or 'clone' in their product listings and advertisements.[139] Dark patterns and fake reviews on e-commerce sites are also used to manipulate consumers' purchasing decisions.[140]

One interviewee has also mentioned the scenario of counterfeit products being introduced into genuine goods supply chains.[141] This occurs when upstream suppliers provide counterfeit goods to unknowing intermediaries, who sell them to other downstream vendors in good faith.[142] Upstream suppliers may also provide mixed batches containing both counterfeits and genuine goods; this approach further conceals the presence of illicit goods.[143]

The offenders behind these fraudulent schemes are generally organised groups or businesses operating from outside the EU, which complicates both enforcement and redress for victims.[144]

Similar to the dissemination of non-delivery scams, survey respondents and interviewees indicate that **social media platforms and e-commerce environments** can function as the primary distribution and marketing infrastructure for counterfeit goods, with platform **advertising tools, content-sharing features, and algorithmic targeting mechanisms** playing a directly enabling role.[145] The extent to which these features act as risk vectors is analysed in Section 3.1.1.

Fraudsters increasingly rely on **ephemeral content formats**, such as stories and live broadcasts on social media, to stream promotional content on a temporary basis, deliberately limiting its traceability and reducing the window available for detection and removal.[146] **Direct messaging functionalities** are used to conduct sales discreetly, while giveaways are exploited to build customer databases for future counterfeit sales.[147] Paid ad placements on

[139] Union des Fabricants (UNIFAB), Counterfeiting & Organised Crime (2025), available at: https://www.unifab.com/wp-content/uploads/2025/06/UNIFAB_Contrefacon-Criminalite_ENGLISH_VDEF_03062025.pdf.

[140] Europol, Internet Organised Crime Threat Assessment 2025 (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf; OECD and EUIPO, Misuse of E-Commerce for Trade in Counterfeits (2021), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/10/misuse-of-e-commerce-for-trade-in-counterfeits_dfd7df43/1c04a64e-en.pdf.

[141] Interview 12.

[142] ibid; Li Fan and Yi Zelong, Counterfeiting and piracy in supply chain management: theoretical studies (2017), available at: https://www.emerald.com/jbim/article-abstract/32/1/98/204136/Counterfeiting-and-piracy-in-supply-chain?redirectedFrom=fulltext.

[143] ibid.

[144] Europol, The other side of the coin – An analysis of financial and economic crime (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/83f3cef9-5769-11ee-9220-01aa75ed71a1/language-en.

[145] Interviews 4, 12; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[146] Union des Fabricants (UNIFAB), Counterfeiting & Organised Crime (2025), available at: https://www.unifab.com/wp-content/uploads/2025/06/UNIFAB_Contrefacon-Criminalite_ENGLISH_VDEF_03062025.pdf.

[147] ibid.

these platforms serve as an additional distribution channel, enabling fraudsters to reach targeted audiences using the same tools available to legitimate advertisers.[148]

Health and wellness scams

Health and wellness scams refer to the online marketing and sale of **unregulated medicines, medical devices or procedures, cosmetics or wellness products**, based on false or misleading claims. Under this category, scammers promote and sell **illegal counterfeit medicines or other harmful and unregulated health products or services**.[149] Reported scams include prescription medication, weight-loss supplements, erectile dysfunction remedies, treatments against diabetes, arthritis, or medical devices such as blood glucose meters.[150]

Deepfakes and AI-fabricated media are used to impersonate health authorities, celebrities, and medical practitioners, while AI-generated imagery promotes weight loss products.[151] Behavioural manipulation follows patterns similar to non-delivery scams, with urgency signals and exploitation of health anxieties.[152] The marketing of these products is perpetrated by criminal networks with flexible structures, as reported by Europol.[153]

As with non-delivery and counterfeit scams, interviewees indicate that social media platforms serve as the primary distribution channel for health and wellness scams, with advertising infrastructure and content-sharing features playing a central enabling role (see Section 3.1.1. for an in-depth assessment).[154]

[148] European Union Intellectual Property Office, Monitoring and analysing social media in relation to IP infringement (2021), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Monitoring_and_analysing_social_media_in_relation_to_IPR_Infringement_Report/2021_Monitoring_and_analysing_social_media_in_relation_to_IPR_Infringement_Report_FullR_en.pdf.

[149] Health Products Regulatory Authority (HPRA), Urgent warning of fraudulent websites and adverts promoting illegal medicines (2025), available at: https://www.hpra.ie/news-events/news/article/urgent-warning-of-fraudulent-websites-and-adverts-promoting-illegal-medicines.

[150] Interview 6; corroborated by AI Forensics, Meta Ads: A Pill Hard to Swallow (2024), available at: https://aiforensics.org/uploads/meta_health.pdf;.

[151] AI Forensics Meta Ads: A Pill Hard to Swallow (2024), available at: https://aiforensics.org/uploads/meta_health.pdf; Check Point, Inside Europe's AI-Fuelled GLP-1 Scam Epidemic (2025), available at: https://blog.checkpoint.com/research/inside-europes-ai-fuelled-glp-1-scam-epidemic.

[152] ACAMS, Fraud and Fear: COVID-19 Scams (2021), available at: https://www.acams.org/en/opinion/fraud-and-fear-covid-19-scams.

[153] Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/The_threat_of_pharmaceutical_crime_in_the_EU_and_beyond.pdf.

[154] Interviews 4, 5.

Fraudsters can exploit social media advertising functionalities to publish fraudulent health product ads at scale, replicating similar content across multiple accounts and EU regions.[155] It is posited that the **reach and targeting precision of social media advertising may enable health scam content to be directed at identifiably vulnerable users** based on their interests or prior engagement with health-related content. This dynamic and the broader phenomenon of health and wellness scams are explored in case study D (Section 6.4).

Hyperlinking functions are also exploited, whereby the displayed URL differs from the actual destination to mislead users into clicking through to fake webshops or cloned websites.[156] Influencers are also leveraged to promote fraudulent wellness products; Europol has noted that **dietary and nutrition influencers have become a primary marketing force behind the sale of illicit hormonal substances.**[157]

Event ticket scams

Event ticket scams concern the **fraudulent online sale of tickets**: victims buy tickets for any type of event requiring an admission ticket, but they either **do not receive anything in return, or they receive fake or stolen tickets**. This scam particularly focuses on **very popular, sold-out events**, relying on the difficulty in obtaining tickets for such events and the openness of fans to pay very high prices for resale tickets from unofficial channels.[158]

Social media platforms and search engines can function as the primary discovery and amplification infrastructure for event ticket scams. As with other e-commerce scams, an interviewee indicated that fraudsters exploit **paid advertising** on social media and search engines to promote fraudulent ticket offers (see Section 3.1.1. for an in-depth assessment).[159] Beyond paid placements, scammers create fake profiles and use groups, pages, and comment sections on posts related to specific events to advertise tickets organically, before transitioning contact to private messaging functions to conduct the sale.[160] **Deficiencies in**

[155] AI Forensics Meta Ads: A Pill Hard to Swallow (2024), available at: https://aiforensics.org/uploads/meta_health.pdf.

[156] ibid.

[157] Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/The_threat_of_pharmaceutical_crime_in_the_EU_and_beyond.pdf; Europol-EUIPO, Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact (2024), accessible at: https://www.europol.europa.eu/publications-events/publications/uncovering-ecosystem-of-intellectual-property-crime.

[158] Europol, Protect yourself from holiday and ticket fraud: From fraudulent flights to non-existing accommodation, holiday fraud is a big business for scammers (2021), available at: https://www.europol.europa.eu/2good2btrue; Bitdefender, Metallica and The Weeknd Fans Targeted in Fake Concert Ticket Scams, Bitdefender Labs Warns (2025), available at: https://www.bitdefender.com/en-us/blog/hotforsecurity/metallica-and-the-weeknd-fans-targeted-in-fake-concert-ticket-scams-bitdefender-labs-warns.

[159] Interview 3.

[160] Take Five, Ticket scams, available at: https://www.takefive-stopfraud.org.uk/protect-yourself/ticket-scams/; this misuse of social media platforms was prevalent in the operation of ticket resale scams during the Paris Summer Olympics in 2024, with the French Gendarmerie noting that 'Facebook, Leboncoin, Telegram and Instagram were often the primary source of resale attempts', as per Franceinfo, Paris 2024 : 338 sites internet frauduleux de revente de billets recensés à quelques semaines du début de la competition (2024), available

content moderation, particularly in comments and groups through which fake tickets are often promoted, may further facilitate this scam type.[161] On search engines, there are documented cases of unauthorised resale platforms appearing prominently in **sponsored placements above organic results** for official ticket sellers, directing users who click the first result to platforms selling false or stolen tickets.[162]

The behavioural model of event ticket scams is also enabled by platform reach: scammers concentrate on high-demand events such as the Olympics or major concert tours, where urgency and scarcity are inherent, and platform amplification ensures fraudulent offers reach large audiences of motivated buyers at precisely the moment of peak demand.[163] The platform role here is distinctive in that the **urgency and scarcity that drive consumer behaviour are inherent to the event market itself rather than fabricated by the scammer**; the platforms' recommender systems merely amplify these pre-existing conditions.

Event ticket scams are perpetrated by a range of offenders from individual social-media-based fraudsters to sophisticated organised crime groups that deploy automated purchasing bots and stolen source codes to acquire tickets at scale.[164]

Subscription scams and hidden renewals

Subscription scams involve fraudulent schemes that **charge victims regularly, typically without their knowledge or explicit consent**. These can take several different forms: free trials with **deliberately unclear or inaccessible cancellation instructions**, hidden contractual terms that impose ongoing charges, and subscription arrangements that are **practically impossible to cancel**, to name just a few.[165] The services involved can be diverse, ranging from IQ tests to PDF editing.[166]

at: https://www.franceinfo.fr/les-jeux-olympiques/paris-2024/info-franceinfo-paris-2024-338-sites-internet-frauduleux-de-revente-de-billets-recenses-a-quelques-semaines-du-debut-de-la-competition_6543401.html.

[161] Interview 3.

[162] For example, FEAT documented Viagogo displaying Google Search ads for the resale of potentially unlawful Radiohead tickets ahead of the official sale, as per FEAT, 1750 Potentially Fraudulent Tickets Offered for Radiohead's European Tour (2025), available at: https://www.feat-alliance.org/2025/09/17/1750-potentially-fraudulent-tickets-offered-for-radioheads-european-tour/.

[163] Surfshark, Beware of concert ticket fraud online (2025), available at: https://surfshark.com/research/chart/concert-ticket-fraud; Nederlandse Politie, Politie waarschuwt met nepwebsite voor ticketfraude (2026), available at: https://www.politie.nl/nieuws/2026/januari/15/politie-waarschuwt-met-nepwebsite-voor-ticketfraude.html.

[164] Surfshark, Beware of concert ticket fraud online (2025), available at: https://surfshark.com/research/chart/concert-ticket-fraud.

[165] Bitdefender, 'Scamscriptions': How to Recognize and Avoid Deceptive Subscriptions (2025), available at: https://www.bitdefender.com/en-us/blog/hotforsecurity/scamscriptions-how-to-recognize-and-avoid-deceptive-subscriptions.

[166] ÖIAT, Verbreitung von Abo-Fallen durch Google Ads (2026), available at: https://www.watchlist-internet.at/fileadmin/files/Abo-Fallen/Google-Policy-Paper.pdf.

Subscription scams and hidden renewals are predominantly perpetrated by commercial entities – including ostensibly legitimate businesses.[167] A further variant involves criminals impersonating reputable companies through fake subscription renewal notices designed to phish for personal and financial data, with compromised accounts subsequently resold on the dark web.[168]

Otherwise, as with other e-commerce scams, fraudsters mainly exploit **paid advertising infrastructure**, purchasing sponsored placements targeting users searching for legitimate services. For example, a 2026 study by ÖIAT found that 43% of flagged subscription scam domains were actively advertised through Google Ads, with 34 problematic advertisers serving nearly 28,000 ads to Austrian users in less than a year alone.[169] This behaviour is facilitated by affordances in the advertising systems of designated services, as discussed below under Section 3.1.1. Promotional links and advertising placements across e-commerce platforms, social media, and news sites are also used to direct users toward services with concealed recurring payment terms.[170]

Dark patterns in this regard play a **central role in subscription scams**, both in inducing the initial sign-up and in discouraging cancellation, for example, through interfaces that make the cancellation process unnecessarily complex, or that present guilt-based or confusing prompts when attempting to terminate the subscription.[171] These techniques are designed to **prolong the subscription so that victims continue to be charged for as long as possible**.

Artificial streaming scams

Artificial streaming scams (or viewbotting) concern the **use of automated processes, like bots or scripts, to manipulate and inflate the engagement rate on streaming services or social media platforms,** with the intent to deceive audiences or advertisers about the popularity of an account or of specific content. The objective of the scammer is to falsely increase their engagement rates to reach monetisation.[172] This scam falls under the e-commerce category, as it negatively impacts the distribution of ad revenue and the reach of paid advertising, influencing commercial relationships. However, it relies on a completely different operational framework than other e-commerce scams. The victimology is also different, as **the damage is externalised to advertisers and other content creators**, rather

[167] US Federal Trade Commission, ICPEN and GPEN, Results of Review of Use of Dark Patterns Affecting Subscription Services (2024), available at: https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-icpen-gpen-announce-results-review-use-dark-patterns-affecting-subscription-services-privacy.

[168] Allstate Identity Protection, Subscription renewal scams, available at: https://www.allstateidentityprotection.com/content-hub/all-about-subscription-renewal-scams.

[169] ÖIAT, Verbreitung von Abo-Fallen durch Google Ads (2026), available at: https://www.watchlist-internet.at/fileadmin/files/Abo-Fallen/Google-Policy-Paper.pdf.

[170] Sheil et al., Staying at the Roach Motel: Cross-Country Analysis of Manipulative Subscription and Cancellation Flows (2024), available at: https://arxiv.org/pdf/2309.17145.

[171] Convington, Digital Fairness Act Series — Topic 4: Digital Subscriptions (2025), available at: https://www.insideprivacy.com/consumer-protection/digital-fairness-act-series-topic-4-digital-subscriptions/.

[172] Nazgol Tavabi et al., Characterizing Activity on the Deep and Dark Web (2019), available at: https://dl.acm.org/doi/pdf/10.1145/3308560.3316502.

than individuals who engage directly with the content posted by perpetrators, as is the case for other e-commerce scams.

Artificial streaming is generally perpetrated by individuals acting on their own, rather than by organised networks – the primary driver is not necessarily the intent to defraud users, but rather the pursuit of monetisation.[173]

Scammers may **exploit the monetisation systems of social media, streaming, and video or music platforms by using artificially generated engagement** (views, likes, comments, and followers) to simulate popularity, unlock performance-based revenue, and improve ranking in search and recommendation results, thereby attracting further authentic viewership.[174] Some civil society representatives claim that performance-based monetisation models directly incentivise inauthentic engagement, creating conditions in which artificial engagement may appear economically rational.[175] This aspect is further explored in Section 3.1.1.

Inauthentic engagement is executed through software scripts ranging from basic viewbotting tools that open content in headless browsers to sophisticated botting services that create fake accounts, mimic logged-in user behaviour, and generate contextually plausible comments or livestream chat replies designed to evade both automated detection and human moderation.[176] One interviewee indicated that the software infrastructure enabling this is commercially available as a product and is actively promoted through publicly accessible courses, substantially lowering barriers to entry and enabling operations at scale.[177]

Insurance scams

Online insurance scams refer to the marketing and sale of **fake insurance policies by intermediaries posing as legitimate insurance brokers** (referred to as 'ghost brokers'). These malicious actors advertise insurance policies on social media, selling victims either **fake or invalid insurance certificates** via fake websites. This scam falls under the e-commerce category, as the victim pays for what they believe to be an authentic service, and the perpetrator delivers in bad faith. This type of scam is singularised through its specific focus on insurance policies. Currently, mainstream reports on online insurance scams mainly come from the United Kingdom and Ireland, where the focus falls on **fraudulent car or house insurance policies marketed through social media**.[178]

Ghost brokers often rely on discounted, too good to be true offers to attract victims. For example, fraudsters dealing in fraudulent car insurance policies mainly target young drivers,

[173] Interview 8.

[174] Andrew Chu et al., Behind the Tube: Exploitative Monetization of Content on YouTube (2022), available at: https://www.usenix.org/system/files/sec22-chu.pdf;

[175] What To Fix, Systemic Risks – Social Media Monetization Systems: A Risk Factor (2025), available at: https://drive.google.com/file/d/1UeKYU3qyeOfEY--oz2hovSpAtx-upOoD/view

[176] StreamCharts, The Hidden Cost of Viewbotting (2025), available at: https://streamscharts.com/reports/viewbotting-whitepaper.

[177] Interview 8.

[178] The Guardian, 'Ghost broking': cut-price car insurance isn't all it seems (2025), available at: https://www.theguardian.com/money/2025/nov/16/ghost-broking-cut-price-car-insurance-scam-watch.

who would generally have to pay higher insurance premiums through legitimate channels.[179] There are three common operational models for insurance scams. Firstly, fraudsters may forge insurance certificates – to that end, the use of generative AI has increased both the scale and cross-border nature of this type of scam, as it has become easier to manipulate documentation and produce very convincing certificates.[180] Secondly, fraudsters who impersonate genuine insurance companies may buy real insurance policies with falsified details to reduce the premium, then share the invalid certificate with the victim.[181] Another option for the fraudster is to still buy a real policy from the company they are impersonating and share it with the victim, but to immediately cancel it afterwards, claiming both the premium refund and the victim's money.[182]

However, reliable data on the type of offender (i.e. sole actors, criminal organisations) behind this type of scam is not yet available.

Insurance scams are primarily marketed through organic social media posts claiming to offer genuine policies at discounted rates, rather than through paid ad placements.[183] The facilitating role of organic content distribution is notable here, and distinguishes this scam from the other e-commerce scam types. Insurance scams exploit the standard post and share mechanics of social media platforms, with scam content amplified by recommender systems.[184] This dynamic is further explored in Section 3.1.1.

Once contact is established, fraudsters migrate communication to private messaging channels to conduct negotiations and deliver fraudulent insurance certificates. Sponsored results on search engines may also be used to promote cloned or AI-generated insurance websites.[185]

Loan and credit offer scams

This type of scam exploits victims' urgent need for financing by presenting fraudulent loan or credit offers disguised as legitimate products. An interviewee indicated that the offers are made particularly attractive through **promises of no credit score or credit history requirements, low interest rates, and overall favourable lending conditions**.[186] Once the victim submits a loan application and receives (fictitious) approval, the fraudsters request the

[179] The Guardian, 'Ghost broking': cut-price car insurance isn't all it seems (2025), available at: https://www.theguardian.com/money/2025/nov/16/ghost-broking-cut-price-car-insurance-scam-watch.

[180] Insurance Europe, Insurance Europe response to EC consultation on online fraud (2026), available at: https://www.insuranceeurope.eu/mediaitem/c356079f-c353-4754-a049-1a0054e0b29b/Insurance+Europe+response+to+EC+consultation+on+online+fraud.pdf?inline=1.

[181] ibid.

[182] ibid.

[183] Insurance Europe, Insurance Europe response to EC consultation on online fraud (2026), available at: https://www.insuranceeurope.eu/mediaitem/c356079f-c353-4754-a049-1a0054e0b29b/Insurance+Europe+response+to+EC+consultation+on+online+fraud.pdf?inline=1.

[184] ibid; Interview 5.

[185] The ABI, Online Fraud, available at: https://www.abi.org.uk/products-and-issues/topics-and-issues/fraud/online-fraud/.

[186] Interview 5.

payment of an upfront fee. After the fee is paid, the scammer disappears, leaving the victim without the promised loan and without any means to recover the lost funds.[187]

Loan and credit offer scams are perpetrated across a spectrum from individual fraudsters to transnational organised crime groups, with the UK National Crime Agency assessing that organised crime groups are 'almost certainly the predominant offenders'; perpetrators are overwhelmingly male, often operate from overseas using fake identities, and deploy increasingly sophisticated infrastructure including fake call centres, cloned websites, and money-muling channels.[188]

The relationship between loan scams and designated services closely mirrors patterns identified in previous e-commerce scam types, with no substantially new platform dynamics introduced.

Fraudsters reach victims through paid advertising and unsolicited direct messages or comments on social media platforms, as well as through manipulated search engine results directing users to fake comparison websites where fraudulent loan schemes are artificially ranked as the best available option.[189] BEUC claims that the presence of illegitimate loan or credit offer advertising on some online platforms would be a **result of lax advertiser verification processes**.[190] The consumer organisation believes that, despite the availability of **online databases maintained by EU authorities that provide public information on companies authorised to provide financial services and products in the EU**, platforms would not systematically check the identity of advertisers against these official registries.[191] BEUC also reports that it has identified multiple ads from non-authorised entities offering credits or loans on TikTok, Facebook, Instagram or Google Search.[192] The role of advertising systems as a risk vector is further described in Section 3.1.1.

Loan and credit scams **disproportionately target individuals in financial distress**; the behavioural profiling capabilities of platform advertising systems may **inadvertently direct such scams toward the most vulnerable users**, who may be identifiable through their search behaviour or engagement with financial hardship content.

[187] L'Autorité de contrôle prudentiel et de résolution (ACPR), L'ACPR met en garde le public contre la multiplication de fausses offres de prêt immobilier ou de rachat de crédit proposées par des individus usurpant l'identité de courtiers et d'établissements de crédit (2024), available at: https://acpr.banque-france.fr/fr/communiques-de-presse/lacpr-met-en-garde-le-public-contre-la-multiplication-de-fausses-offres-de-pret-immobilier-ou-de.

[188] UK Government, National Assessment Centre Fraud Assessment 2025 (2025), available at: https://www.gov.uk/government/publications/national-assessment-centre-fraud-assessment-2025/national-assessment-centre-fraud-assessment-2025.

[189] Interviews 2, 4; Financial Services and Market Authority, Received an interesting credit offer? Be careful! (2025), available at: https://www.fsma.be/en/warnings/received-interesting-credit-offer-be-careful.https://www.fsma.be/en/warnings/received-interesting-credit-offer-be-careful.

[190] BEUC, Sponsored by Scammers (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf.

[191] ibid.

[192] ibid.

Rental scams

Rental scams typically involve **listing a non-existent or misrepresented property**, impersonating a host or landlord, and **collecting upfront payments from victims**. This type of scam takes two main forms. In one format, scammers set up false identities and advertise non-existent accommodations. In the other, they **hijack genuine accounts**, using them to attract victims and to redirect them to fraudulent payment links.

When new accounts are set up, perpetrators follow different narratives, depending on the type of rental proposed to victims. In the context of vacation rentals, fraudsters create listings on dedicated accommodation platforms, complete with stolen pictures and exaggerated descriptions. Once the consumer reaches out to book the property, the host prompts them to complete the upfront payment off the platform; after payment is made, the fake host becomes impossible to reach.[193] Alternatively, on the day of check-in, the fake host contacts the guests to inform them that the property is no longer available, sometimes offering lower-quality alternative accommodation.[194] In the context of longer-term rentals, the fraudster impersonates a landlord and persuades the victim to pay a deposit for a property they have never visited, and most likely does not exist. This scheme qualifies as a form of advance fee fraud.[195]

Respondents to the survey indicated that fraudulent listings are sometimes taken offline the moment the victims realise they have been scammed and seek redress.[196] However, research from Which? also found that Booking.com hosted multiple listings with 'hundreds of negative reviews' that claimed the accommodation was a scam.[197] The consumer organisation also claims that some of the listings were not removed, even after it reported them to the platform. Moreover, Which? points out that individual users are shown a selection of reviews identified as 'most relevant' for them – in this instance, none of the reviews warning of the fraudulent nature of the listings were surfaced to users, unless they manually changed the ranking system from 'most relevant' to 'newest'.[198]

Distribution channels vary by rental type. Vacation rental scams are primarily conducted through major booking and accommodation platforms, while longer-term rental scams rely more on dedicated housing websites and social media platforms, where listings can be posted with minimal verification.[199] The scammers rely on basic operational techniques, such as

[193] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[194] Julie Reid, Delusive speech in the sharing economy: Scam Inc. (2025), available at: https://www.taylorfrancis.com/books/mono/10.4324/9781003513995/delusive-speech-sharing-economy-julie-reid.

[195] Sophie Van Der Zee et al., The gift of the gab: Are rental scammers skilled at the art of persuasion? (2019), available at: https://arxiv.org/abs/1911.08253.

[196] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[197] Which?, The scam crisis on Booking.com (2025), available at: https://www.which.co.uk/news/article/the-scam-crisis-on-booking.com-aAj2P4i2c06f; Which?, What went wrong with Booking.com? (2025), available at: https://www.which.co.uk/news/article/what-went-wrong-with-booking.com-aYOyv4Q7Ua2D.

[198] ibid.

[199] Julie Reid, Delusive speech in the sharing economy: Scam Inc. (2025), available at: https://www.taylorfrancis.com/books/mono/10.4324/9781003513995/delusive-speech-sharing-economy-

impersonation of real hosts, theft of photographs and listing details, and persuasion through mimicry of genuine communication styles.[200]

The second format of rental scams involves compromising legitimate host or hotel accounts through phishing, malware, or credential theft targeting accommodation provider staff.[201] Once access is obtained, fraudsters operate from within the platform's trusted environment, using official in-app messaging systems to contact guests with accurate reservation details before directing them to cloned payment pages or external channels to complete a fraudulent transaction.[202]

A case documented by Altroconsumo in 2025 exemplifies this: fraudsters gained access to victims' Booking.com reservation data and directed them to a cloned version of the platform that mirrored the exact dates and details of their real bookings, prompting re-entry of payment information.[203] Scammers compromised hosts' or hotels' Booking.com accounts by harvesting their credentials through phishing emails or malware, then accessing reservation data to interact with guests through the Booking.com messaging system.[204] From there, victims were prompted to verify payment details, confirm their reservation, or resolve alleged issues to avoid cancellation, being redirected through embedded links or follow-up instructions to cloned websites or fraudulent payment pages.[205] Victims were also encouraged to move to external communication channels where the fraudulent transaction was completed.[206]

There is limited publicly available information on the offender profile associated with rental scams, potentially indicating a **gap in available data**. The facilitating role of platforms here goes **beyond the advertising and ranking dynamics** identified in previous scam types. The architecture of acommodation platforms (**internal messaging systems, verified account environments and data-rich reservation records**) can become the instrument of a scam when accounts are compromised. The **effectiveness of the scam is directly proportional to the platform's own credibility**: messages sent through official channels referencing accurate booking data are credible precisely because the platform has established that trust with users. Moreover, it can be posited that the interface of a rental accommodation platform,

julie-reid; Sophie Van Der Zee et al., The gift of the gab: Are rental scammers skilled at the art of persuasion? (2019), available at: https://arxiv.org/abs/1911.08253.

[200] ibid.

[201] Malwarebytes, Booking.com breach gives scammers what they need to target guests (2026), available at: https://www.malwarebytes.com/blog/data-breaches/2026/04/booking-com-breach-gives-scammers-what-they-need-to-target-guests.

[202] Norton, Reservation Hijack Scam: the travel scam that looks exactly like your real hotel booking (2026), available at: https://us.norton.com/blog/online-scams/reservation-hijacking-scam.

[203] Altroconsumo, Prenotazioni su Booking.com: occhio alla truffa del sito clone (2025), available at: https://www.altroconsumo.it/soldi/truffe/news/truffa-sito-booking-clone.

[204] Malwarebytes, Booking.com breach gives scammers what they need to target guests (2026), available at: https://www.malwarebytes.com/blog/data-breaches/2026/04/booking-com-breach-gives-scammers-what-they-need-to-target-guests.

[205] Norton, Reservation Hijack Scam: the travel scam that looks exactly like your real hotel booking (2026), available at: https://us.norton.com/blog/online-scams/reservation-hijacking-scam.

[206] ibid.

which presents a continuous list of available accommodations, can allow for **fraudulent postings to blend in with the legitimate ones**.

2.4. Employment and collaboration scams

Employment and collaboration scams are fraudulent schemes in which criminals pose as employers, recruiters, or business collaborators to deceive victims into believing they have secured a legitimate job or commercial opportunity. The following paragraphs differentiate between three types, with fake job scams as the main category, and money mule recruitment and DM to Collab bots singularised through their specific contexts.

Fake job scams

Fake job scams entail the online advertising of **false job positions by fraudsters impersonating recruiters**, with the aim of **stealing victims' personal information and of obtaining money illegally** from them.[207] As part of this scam, victims are offered a job and then asked to pay different charges for the recruitment and onboarding process; these may relate to, *inter alia*, administrative costs, background check costs, and management costs. This approach can be considered the traditional structure for online employment scams and is often perpetrated by **criminal organisations to collect personal data** to use for further criminal purposes, but also for financial incentives.[208] Importantly, this category is different from 'money mule recruitment' scams (discussed in the subsequent section), where the job advertised is illegal or associated with illegal behaviour.

The specific infrastructure of online recruitment sites gives fraudsters an advantage, as their **fraudulent job postings blend in with the legitimate ones**, rendering it hard to detect job scams.[209]

Scammers rely on basic operational tools such as impersonation, i.e., pretending to be a representative of a legitimate company or of a recruitment agency. They often make offers that are too good to be true, promising high incomes, little effort, or no specific qualifications needed. They take advantage of victims' desperation, vulnerable economic situation, or pressing need to find a job, promising a quick hiring process that does not require interviews or references from previous employers.[210] They also pressure victims into acting quickly, requiring fast decisions and generating a sense of urgency.

---

[207] Srivani Putta et al., Machine Learning Approach for Fake Job Ad Prediction (2023), available at: https://www.proquest.com/openview/00c88ab1a6b7334de114d32519cfae08/1?pq-origsite=gscholar&cbl=2045096.

[208] Cassandra Cross and Deanna Grant-Smith, Recruitment Fraud: Increased opportunities for exploitation in times of uncertainty? (2022), available at: https://socialalternatives.com/wp-content/uploads/2022/02/CrossGrant-Smith-SA40-4.pdf.

[209] Syed Mahbub and Eric Pardede, Using Contextual Features for Online Recruitment Fraud Detection (2018), available at: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1247&context=isd2014.

[210] Alexandrea J Ravanelle et al., Good jobs, scam jobs: Detecting, normalizing, and internalizing online job scams during the COVID-19 pandemic (2022), available at: https://journals.sagepub.com/doi/pdf/10.1177/14614448221099223.

Although fake job scams are commonly perpetrated by criminal organisations, the accessibility of online recruitment platforms also enables individual actors to engage in this type of fraud.[211] Reliable data on the geographic distribution of offenders remains limited; however, the operational characteristics of these scams, including the use of identity obfuscation techniques and the targeting of victims across multiple jurisdictions, suggest patterns consistent with the transnational organised crime networks identified in other scam types. The involvement of both organised structures and opportunistic individuals reflects the low barriers to entry afforded by digital recruitment environments.

Fake job scams are primarily disseminated through **recruitment platforms**.[212] **Low barriers to account creation**, combined with self-declaration-based identity verification, may allow fraudsters to establish credible recruiter profiles using false or stolen information.[213] The **professional networking architecture provides visibility into potential victims' employment status, career aspirations, and financial circumstances**.[214] For example, it is posited that the '#open to work' profile graphic may increase the likelihood of being approached by scammers.[215] Scammers post fake job openings or directly contact victims with job offers.

Money mule recruitment

Money mule recruitment scams refer to the use of job adverts to **recruit individuals for money muling**, a criminal practice used to **move funds resulting from illicit sources**, some even from the operation of other financial scams described in this report. As part of this scam, victims are asked to **receive and transfer funds into different bank accounts or withdraw them in cash** and wire them to the scammer.[216] The victims **do not know they are participating in a criminal operation** and often believe they are merely carrying out an ordinary job as a money transfer agent.[217] This type of scam is perpetrated by **large criminal organisations as part of a broader net of fraudulent or illicit activities**, the objective of

[211] UK Home Office, National Assessment Centre - Fraud assessment 2025 (2025), available at: https://www.gov.uk/government/publications/national-assessment-centre-fraud-assessment-2025.

[212] Vice, Scammers Are Sending Fake Job Offers on LinkedIn (2021), available at: https://www.vice.com/en/article/scammers-are-sending-fake-job-offers-on-linkedin/.

[213] Navid Ayoobi et al., The Looming Threat of Fake and LLM-generated LinkedIn Profiles: Challenges and Opportunities for Detection and Prevention (2023), available at: https://dl.acm.org/doi/pdf/10.1145/3603163.3609064.

[214] Forbes, Job Seekers: Be Careful Using LinkedIn's New "Open To Work" Feature (2020), available at: https://www.forbes.com/sites/roberthellmann/2020/07/20/job-seekers-be-careful-using-linkedins-new-open-to-work-feature/.

[215] ibid.

[216] Muhammad Subtain Raza et al., Role of money mules in money laundering and financial crimes a discussion through case studies (2020), available at: https://ideas.repec.org/a/eme/jfcpps/jfc-02-2020-0028.html.

[217] Mohd Irwan Abdul Rani et al., Exploring Money Mule Recruitment: An Initiative in Combating Money Laundering (2023), available at: https://www.researchgate.net/profile/Salwa-Zolkaflil/publication/369823521_EXPLORING_MONEY_MULE_RECRUITMENT_AN_INITIATIVE_IN_COMBATING_MONEY_LAUNDERING/links/642e34354e83cd0e2f93f7b7/EXPLORING-MONEY-MULE-RECRUITMENT-AN-INITIATIVE-IN-COMBATING-MONEY-LAUNDERING.pdf.

recruiting the money mules being to generate distance between the core criminal network and the funds.

In some cases, the victim may be compensated for carrying out the tasks (e.g. through a commission fee from the funds moved), but that is not a prerequisite. The fraudulent character of this scam primarily stems from creating the illusion that the victims are genuinely employed for a legitimate purpose. It is important to note that money mule recruitment can be perceived both as a scam in itself (towards the recruited mules), but also as an operational tool for laundering the funds unfairly earned through other illicit behaviours, including financial scams.

Money mule recruitment scams primarily rely on **social engineering techniques**, promising high financial compensation and normalising this behaviour as a safe or reliable opportunity for collaboration.[218]

Money mule recruitment scams are often perpetrated through job adverts on recruitment websites or social media posts promising quick money.[219] Offenders also create false profiles to join popular groups or interact with special interest pages to identify potential victims.[220] Social media platforms may facilitate this through organic content distribution and structural features such as groups, pages and profile discovery tools.[221] After recruitment, communication moves to encrypted messaging apps. The platform affordances that facilitate this type of scam are further discussed in Section 3.1.1.

Direct Message (DM) to Collab bots

This type of scam involves fraudulent sponsorship or collaboration offers sent to content creators, with **offenders impersonating legitimate brands, agencies, or talent management companies**. Victims are typically asked to pay upfront for shipping costs, product samples, or promotional materials as a precondition for the collaboration. Once the payment is made, the fraudster's profile disappears, and no further contact is possible.[222] On

[218] UK Finance, Money mule recruiters use fake online job adverts to target "Generation Covid", available at: https://www.ukfinance.org.uk/press/press-release/money-mule-recruiters-use-fake-online-job-adverts-to-target-generation-covid.

[219] Europol, Money Muling (2025), available at: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling; Ehi Eric Esoimeme, Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules (2021), available at: https://www.emerald.com/jmlc/article-abstract/24/1/201/241861/Identifying-and-reducing-the-money-laundering?redirectedFrom=fulltext.

[220] LMJ Bekkers and ER Leukfeldt, Recruiting money mules on Instagram: a qualitative examination of the online involvement mechanisms of cybercrime (2022), available at: https://www.tandfonline.com/doi/full/10.1080/01639625.2022.2073298.

[221] LMJ Bekkers and ER Leukfeldt, Recruiting money mules on Instagram: a qualitative examination of the online involvement mechanisms of cybercrime (2022), available at: https://www.tandfonline.com/doi/full/10.1080/01639625.2022.2073298.

[222] Bitdefender, How to Spot and Avoid Sponsorship Scams (2024), available at: https://www.bitdefender.co.uk/consumer/support/answer/107805/.

top of this, the products ordered are often not delivered or are of extremely low quality compared to what was originally promised.[223]

DM to Collab scams are primarily perpetrated through **automated systems and bot networks**, which enable fraudsters to contact large numbers of content creators with minimal effort. While the operators behind these bot networks remain largely unidentified in available literature, the scale and automation of these operations suggest involvement by organised actors with technical capabilities. The low barrier to entry for creating fake accounts and deploying bots means that both individual fraudsters and more sophisticated criminal networks may engage in this type of scam. Geographic attribution remains difficult due to the use of anonymising technologies and the cross-border nature of social media platforms.

This scam operates through **social media platforms**, with scammers luring users into getting in touch with them, either through account descriptions containing 'DM me' hashtags or uploading posts or comments with the same hashtag.[224] The scam relies on **public-facing bait, disseminated to a wide audience.** To appear legitimate, scammers use strategies such as writing 'official' in their username or claiming to be certified professionals.[225] Victims are then lured to migrate to the private messaging environment, where direct messaging features allow fraudsters to interact with creators with minimal effort or cost.[226]

As this scam is primarily disseminated through bots and fake accounts, it is facilitated through easy-to-navigate account creation processes on social media, with limited identity verification requirements; this aspect is further described in Section 3.1.1. Unlike the standard cross-platform migration model observed in most other scam types, victims are rarely redirected to an external fraudulent destination; the fraudulent payment is solicited directly within the messaging environment of the social media platform.

2.5. Unexpected gain scams

Unexpected gain scams (also called 'unexpected winnings' or 'money scams') are based on the **promise of receiving an unanticipated financial reward or prize**, such as cash, vehicles, electronics, or holidays. Victims are typically informed that they have won or are entitled to a benefit and are then required to **pay an upfront fee framed as taxes, administrative costs, or processing charges**, to access the funds or claim the prize. In addition to financial gains, these scams are frequently used to **obtain personal data, which may subsequently be exploited for further fraudulent activities**.[227]

The sub-sections below list some specific types of unexpected gain scams:

---

[223] VICE, Those 'DM to Collab' Instagram Messages Are Probably a Scam (2021), available at: https://www.vice.com/en/article/dm-to-collab-instagram-messages-scam/.

[224] Raj Vardhan et al., #DM-Me: Susceptibility to Direct Messaging-Based Scams (2023), available at: https://dl.acm.org/doi/pdf/10.1145/3579856.3582815.

[225] ibid.

[226] Raj Vardhan et al., #DM-Me: Susceptibility to Direct Messaging-Based Scams (2023), available at: https://dl.acm.org/doi/pdf/10.1145/3579856.3582815.

[227] ScamWatch, Unexpected money scams, available at: https://www.scamwatch.gov.au/types-of-scams/unexpected-money-scams

- **Fake contests, raffles and prize scams** involve scammers convincing victims that they have won a prize, a competition or a giveaway. Victims are then requested to provide personal or financial information or to pay an upfront fee to claim the purported prize. These schemes are designed to extract sensitive data or obtain payments under false pretences.[228]
- **Inheritance, donation, and lottery scams** typically begin with an unexpected message or call informing the victim that they are entitled to a large sum of money. This may be framed as an inheritance from an unknown relative, a donation, or lottery winnings.
- **Gambling scams** are a form of online scam in which victims are deceived into participating in fraudulent gambling activities, such as fake online casinos, sports betting services, or gaming platforms. Offenders typically promote these schemes by claiming to offer privileged access, guaranteed winnings, or supposedly reliable betting systems. In practice, victims are encouraged to deposit funds on these platforms, often starting with small amounts to reduce suspicion.[229] However, the platforms are manipulated so that losses are inevitable, and any displayed winnings are fictitious. When victims attempt to withdraw funds, scammers either block the transaction, freeze the account, or impose fabricated conditions that prevent payouts. As a result, victims are unable to recover their deposits or any purported earnings.[230]
- **Rebate scams** involve false claims that the victim is entitled to a refund or compensation from a government authority, financial institution, or other trusted organisation. This may relate to overpaid taxes, bank charges or other fees, or to the purported recovery of funds lost in a previous scam. Offenders may impersonate public authorities, law enforcement agencies or financial institutions and claim that compensation is available, provided the victim first pays administrative or processing fees, supplies personal or financial information, or follows other fraudulent instructions. The objective is to obtain additional money or sensitive information by exploiting the victim's trust in the purported organisation.[231]
- **Online penny auction scams** involve platforms where users are required to pay a non-refundable fee for each bid placed on an item. While the advertised prices may appear attractive, participants often incur high costs through repeated bidding without successfully obtaining the item.[232]

Unexpected gain scams are perpetrated by a range of actors, from individual opportunistic fraudsters to organised cybercrime networks. The operational simplicity of advance-fee mechanisms means that these scams can be conducted by sole actors with minimal technical

[228] ScamWatch, Unexpected money scams, available at: https://www.scamwatch.gov.au/types-of-scams/unexpected-money-scams.

[229] Geng Hong et al., Analyzing Ground-Truth Data of Mobile Gambling Scams (2022), available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9833665; Gendigital, Gen Q3/2025 Threat Report (2025), available at: https://www.gendigital.com/blog/insights/reports/threat-report-q3-2025.

[230] Interview 6.

[231] ScamWatch, Unexpected money scams, available at: https://www.scamwatch.gov.au/types-of-scams/unexpected-money-scams.

[232] ibid; Markou Christiana, Online penny auctions and the protection of the consumer under EU law (2014), available at: https://www.sciencedirect.com/science/article/abs/pii/S0267364914001290

infrastructure.[233] However, larger-scale operations, particularly those involving fraudulent gambling platforms or sophisticated fake lottery schemes, are typically run by organised criminal groups.[234] The cross-border nature of these scams, combined with the use of anonymising technologies and cryptocurrency payment mechanisms, complicates geographic attribution and law enforcement efforts.

Unexpected gains scams rely heavily on platform infrastructure for distribution, with advertising systems and private messaging functions playing a particularly central role. One interviewee indicated that the **promise of free money or prizes is particularly effective in the fast-scrolling, high-stimulus environment of social media feeds**, where algorithmic amplification of engaging content further extends the reach of fraudulent offers.[235]

Paid advertising is a primary distribution mechanism, particularly for gambling scams, fake contests, and online penny auction scams.[236] These ads employ deceptive creative tactics: AI-generated deepfakes impersonating public figures, fabricated news segments, and mimicry of trusted brands.[237] Pop-up windows and interactive elements are also used to draw users into advance-fee mechanisms or prompt disclosure of financial details.[238] The facilitating role of advertising infrastructure is discussed further in Section 3.1.1.

A feature specific to this context is the jurisdictional dimension: **platform advertising systems may enable unlicensed gambling operators to illegally promote services to users in countries where they hold no valid licence**; this could expose users to unregulated platforms without any platform-level verification of operator licensing status.[239]

Scammers also leverage the direct messaging functions of online platforms to disseminate their scams, particularly in relation to fake contests, raffles and prize scams, inheritance, donation, lottery scams and rebate scams.[240] The absence of high-assurance identity

[233] Janine Ungvarsky, Advance-fee Scams (2023), available at: https://www.ebsco.com/research-starters/law/advance-fee-scams#full-article.

[234] UN Office on Drugs and Crime, Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape (2024), available at: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

[235] Interview 9.

[236] Analysis by Debunk.org found that 99% of gambling scam cases involved ads, with scammers setting up platform pages and immediately placing ads targeting any country and language, as per: Debunk, Debunk.org Trusted Flagger 2025 Report (2026), available at: https://www.debunk.org/debunk-org-trusted-flagger-2025-report.

[237] ibid.

[238] ibid.

[239] ibid.

[240] Safeonweb, Beware of inheritance fraud: reports of unexpected inheritances are doing the rounds again (2025), available at: https://safeonweb.be/en/news/beware-inheritance-fraud-reports-unexpected-inheritances-are-doing-rounds-again; US Internal Revenue Service, IRS assesses $162 million in penalties over false tax credit claims tied to social media (2025), available at: https://www.irs.gov/newsroom/irs-assesses-162-million-in-penalties-over-false-tax-credit-claims-tied-to-social-media; Scamwatch, Beware of fake lottery and competition 'wins' on social networking platforms (2015), available at:

verification at account creation enables fraudsters to impersonate institutions and to send messages purporting to come from legal representatives, banks, or foreign officials. These risk vectors are assessed in-depth in Section 3.1.1.

Beyond social media, fraudsters also place **fake applications on legitimate app stores**, particularly as part of gambling scams, exploiting the trust conferred by official distribution platforms.[241] Research by Trend Micro documented hundreds of fake applications on both the Apple App Store and Google Play, where apps are submitted with innocuous descriptions inconsistent with their actual content and are capable of transforming into gambling interfaces once installed, exploiting user trust in curated marketplaces.[242] The primary evasion technique involves a form of **delayed activation or 'switch' mechanism**: developers submit a policy-compliant application for review and, once approved, remotely enable hidden gambling functionality, thereby circumventing both automated and human review processes.[243] This is sometimes achieved through server-side toggles or post-review code injection via frameworks such as CodePush.[244]

2.6. Charity and disaster relief scams

Charity and disaster relief scams are fraudulent schemes in which criminals solicit donations from the public, typically exploiting moments of heightened public empathy such as natural disasters, armed conflicts, or humanitarian crises. Victims are deceived into believing their contributions will support genuine relief efforts, while funds are instead diverted for the personal gain of the fraudsters.

Charity scams

With charity scams, fraudsters **exploit crises or natural disasters** to pose as charity organisations and obtain donations. Such scams have been observed in particular in the context of the COVID-19 pandemic, the Russian invasion of Ukraine, earthquakes in Türkiye and Syria, or the floods in Spain.[245] The **speed with which fraudulent charity campaigns**

https://www.scamwatch.gov.au/about-us/news-and-alerts/beware-of-fake-lottery-and-competition-wins-on-social-networking-platforms.

241 Interview 6; Geng Hong et al., Analyzing Ground-Truth Data of Mobile Gambling Scams (2022), available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9833665.

242 TrendMicro, 'Hundreds of Fake Apps in iOS App Store and Google Play' (2019), available at: https://www.trendmicro.com/en_us/research/19/i/gambling-apps-sneak-top-100-hundreds-fake-apps-spread-app-store-google-play.html. .

243 ibid; Filipe Espósito, 'A deep dive into how developers trick App Store review into approving malicious apps' (2024), available at: https://9to5mac.com/2024/08/02/developers-trick-app-store-review/.

244 ibid.

245 Europol, Internet Organised Crime Threat Assessment (IOCTA) (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/238c0013-26a9-11ee-a2d3-01aa75ed71a1/language-en

emerge following major disasters suggests that **fraudsters have a degree of operational preparedness** to exploit platform virality at moments of peak empathy.[246]

The use of impersonation techniques, fake websites, and manipulated payment channels indicates that perpetrators possess a certain level of technical sophistication.[247] However, the relatively low barriers to creating fraudulent charity appeals on social media also enable individual actors to engage in this type of scam on a smaller scale.[248]

Charity scams exhibit a direct relationship with platform infrastructure, with **organic content distribution and algorithmic amplification** playing enabling roles. An interviewee indicated that fraudsters distribute campaigns impersonating legitimate organisations primarily through organic social media posts.[249] As charity scams focus on high-urgency stories, scammers **exploit recommender systems to reach large audiences at moments of heightened public empathy**. The **absence of systematic verification of charitable organisation credentials** means fraudulent campaigns benefit from the same reach as legitimate ones.

Fraudulent crowdfunding campaigns

Fraudulent crowdfunding campaigns pretend to conduct legitimate fundraising efforts for a wide range of causes, such as humanitarian action, emergency aid (especially following natural disasters such as floods, earthquakes, fires), or personal projects.[250] Scammers pretend to be victims or to collect money for a cause. Some use fictitious (usually life-threatening) illnesses to attract donors. Crowdfunding scams are also used to support projects that never actually come to fruition.[251]

Crowdfunding scams closely mirror the dynamics identified in charity scams but introduce an additional and structurally significant dimension: scams conducted not merely through impersonation of legitimate platforms, but directly *on* legitimate crowdfunding platforms themselves. Operational methods mirror those identified in charity fraud: imitation campaigns, impersonation of legitimate charities or public figures, phishing, and identity theft, combined with compelling imagery and emotionally manipulative narratives aligned with trending crisis events to maximise visibility and empathy-driven engagement.[252]

---

[246] Rasha Kassem, The dark side of giving: Exposing charity fraud (2025), available at: https://www.acfe.com/fraud-magazine/all-issues/issue/article?s=2025-marapr-charity-fraud-dark-side-giving.

[247] ibid.

[248] ibid.

[249] Interview 1.

[250] Hackers Rangers, Scams Involving Crowdfunding Campaigns and Fake Donations: How Can You Protect Yourself?, available at: https://hackerrangers.com/scams/scams-involving-crowdfunding-campaigns-and-fake-donations/

[251] Okta, Crowdfunding Scams: How to Spot Them and Stay Safe (2024), available at: https://www.okta.com/identity-101/crowdfunding-scams/

[252] Hackers Rangers, Scams Involving Crowdfunding Campaigns and Fake Donations: How Can You Protect Yourself?, available at: https://hackerrangers.com/scams/scams-involving-crowdfunding-campaigns-and-fake-donations/.

Fraudulent crowdfunding campaigns are conducted by both individual actors and organised groups. The accessibility of crowdfunding platforms, combined with limited identity verification requirements, enables opportunistic individuals to launch deceptive campaigns with minimal effort.[253] At the same time, more sophisticated operations, particularly those involving coordinated impersonation of legitimate charities or systematic exploitation of multiple disaster events, suggest involvement by organised actors, as the United States Financial Crimes Enforcement Network reports that crowdfunding platforms may be used by criminal organisations for money laundering.[254] Available evidence does not point to specific geographic concentrations of offenders; however, the cross-border reach of crowdfunding platforms and social media enables perpetrators to target donors across multiple jurisdictions while operating from locations with limited regulatory enforcement.

Designated services play an important facilitating role in the dissemination and reach of fraudulent crowdfunding campaigns. Fraudsters frequently use social media platforms to promote fraudulent campaigns. The facilitating role of algorithmic amplification of trending and high-urgency content identified in the charity scam context equally applies. Fraudsters frequently distribute fraudulent campaigns through organic social media posts before redirecting users towards external crowdfunding pages. The role of these functions in scam dissemination is further described in Section 3.1.1.

However, scams are also **conducted directly on genuine crowdfunding platforms**. This characteristic renders crowdfunding scams **structurally distinct from charity scams** in one critical respect: the scam operates directly within a legitimate transactional platform rather than redirecting victims to an external fraudulent website. This means the **platform's own trust signals** (verified project pages, donation progress bars, social sharing indicators, and platform branding) **are co-opted to lend credibility to the fraud**.[255] To that end, scammers exploit the **low-friction onboarding, limited legal disclosure requirements, and weak identity verification processes** of these crowdfunding platforms to rapidly create fake personas and launch campaigns during disaster windows.[256]

[253] Mokter Hossain and Steven A. Creek, Unveiling and Brightening the Dark Side of Crowdfunding (2021), available at: https://cmr.berkeley.edu/assets/documents/pdf/2021-09-unveiling-and-brightening-the-dark-side-of-crowdfunding.pdf.

[254] United States Financial Crimes Enforcement Network, FinCEN Advisory FIN-2017-A007 (2017), available at: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a007-0.

[255] Seunghun Lee et al., Fraud Detection on Crowdfunding Platforms Using Multiple Feature Selection Methods (2025), available at: https://xplorestaging.ieee.org/ielx8/6287639/10820123/10909102.pdf?arnumber=10909102&utm_source=scopus&getft_integrator=scopus.

[256] ibid.

3. Operationalisation of online financial scams on online platforms

Online financial scams have become a widespread phenomenon across the European Union. The following paragraphs briefly take stock of the available data on prevalent types of online financial scams – in this regard, a disclaimer is warranted, as there are limited publicly available statistics or estimates. Then, this section focuses on the risk factors related to the design and functioning of VLOPs and VLOSEs. This assessment is followed by a discussion on the cross-platform migration patterns underlying online financial scams, and the adaptation behaviours observed in scammers. The following sections then compile and present the most common operational tools and social engineering methods used by scammers, with a dedicated section on the role of artificial intelligence in amplifying and scaling online scams. The concluding section briefly focuses on external factors facilitating online financial scams, such as fraud-as-a-service infrastructures.

A number of recurrent scam types are considered most prevalent, with interviewees indicating that **investment-related scams are among the most frequently encountered types of financial scams**.[257] In fact, investment scams, and especially those variants linked to cryptocurrencies, have seen a **marked increase in recent years**.[258] This assessment is supported by survey data, with investment scams being identified by **the most respondent Member States (11)** as one of the scam types most commonly encountered by consumers.[259]

Alongside investment scams, non-delivery of goods, notably through fake online shops, represents another highly prevalent category, as reported by 11 Member States.[260] National evidence illustrates the scale of this phenomenon: the Dutch national hotline for online scams (LMIO) expected approximately 14,000 reports in 2023 concerning online stores that failed to deliver purchased items, with approximately 10,000 victims reporting having been misled through Instagram.[261]

Other scam types, such as credit and loan fraud, are reported less frequently, but remain consistently present across jurisdictions, as indicated by multiple interviewees.[262] Their prevalence appears to be more context-dependent and linked to specific consumer needs or economic conditions.

In fact, beyond overall prevalence, the occurrence of scam types tends to **reflect temporal and contextual patterns**. Several survey respondents report **seasonal variations**, with

[257] Interviews 2, 4, 5.

[258] Interview 1; Better Finance, Unmasking Digital Deception: A Data-Driven Approach to Mapping and Combating Online Investment Fraud in Europe (2024), available at: https://betterfinance.eu/publication/unmasking-digital-deception-a-data-driven-approach-to-mapping-and-combating-online-investment-fraud-in-europe/

[259] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[260] ibid.

[261] Autoriteit Consument en Markt, Consumer organizations warn against untrustworthy online stores (2023), available at: https://www.acm.nl/en/publications/consumer-organizations-warn-against-untrustworthy-online-stores.

[262] Interviews 4, 5.

certain scams intensifying during specific periods.[263] For example, **shopping-related scams tend to increase during major events** such as Black Friday and the Christmas season, when increased intention to purchase and time pressure, paired with a disposition to believe lower prices, create favourable conditions for scams to proliferate.[264] Similarly, **credit and loan scams are reported to be more visible** in the above-mentioned periods, due to the consumers' need for increased funds.[265] Among those Member States that reported seasonal patterns in their survey response, the majority observed **spikes in travel-related rental scams over the summer months**, increased impersonation of financial institutions during the tax filing season, and, to a lesser extent, scam schemes exploiting political figures in the periods leading up to elections.[266]

Taken together, these patterns indicate that the prevalence of financial scams in the EU is not only shaped by the characteristics of individual scam types, but also by how these scams are deployed across different platforms and user contexts. The following sections therefore examine how scammers exploit specific platform features when operationalising scam schemes, including references to the connection between specific features and different scam types.

3.1. Platform features as financial scam dissemination channels

This section focuses on platform design and features as risk factors which are leveraged by fraudsters, and which are conducive to the operationalisation of online financial scams. It first focuses on third-party data on the role of platform features in the unfolding of online financial scams and then summarises and identifies trends in the dissemination vectors as identified by VLOPs and VLOSEs, on the basis of their Risk Assessment Reports from 2025. This delineation allows for a comparison between the two perspectives, potentially underscoring new avenues for empirical research.

3.1.1. Overview of risk factors identified by third parties

The operation of online financial scams is often facilitated through the design, features, or functioning of online platforms and search engines, allowing scammers to exploit these environments as vectors for the dissemination of scams. The following paragraphs assess each of the identified risk factors and their role in the online financial scam cycle.

Advertising systems

Based on the stakeholder consultation and available literature, **paid advertising space** is one of the most commonly identified vectors through which online financial scams are

[263] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[264] Interviews 4, 7; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[265] ibid.

[266] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

disseminated online**.** Ad placements are used in the dissemination of a wide range of scam types identified in this report; *inter alia,* investment scams, undelivered products or counterfeit scams, health and wellness scams, event ticket scams, subscription scams, loan or credit offer scams, and unexpected gain scams.

Unlike organic content, ad placement guarantees prominence and high visibility, significantly amplifying the exposure of users to advertising content. Interviewees and survey respondents indicated that this amplified reach is maliciously leveraged by scammers, who rely on paid advertising as an easily scalable initial contact point with victims.[267] The design and functioning of advertising systems may also facilitate scammers' reliance on ad placements as an initial contact point with victims.

As part of the stakeholder consultation, it was indicated that the reach and impact of fraudulent advertising are primarily a result of volume, rather than of activity or engagement rates.[268] Many fraudulent ads are active for very short periods (~1-2 days), without reaching significant engagement rates, meaning that scammers prefer relying on **mass spamming of lower-engagement fraudulent ads**, with the aggregated effect of reaching high volumes of users.[269] Research conducted by vzbv found that 50% of the 653 fake webshops the association has monitored were advertised via Facebook, Instagram or Google's designated services, with the five most wide-reaching shops alone gaining 134 million ad impressions on Google platforms.[270] Similar research from Austria identified 246 fraudulent ads on Facebook and Instagram impersonating Austrian celebrities to promote investment scams over the course of two days; those 246 ads alone reached around 200,000 people per day.[271] Across an extended timeline (January to April 2024), the same study identified over 9,000 such fraudulent ads.[272]

The Irish Central Bank reports that 1 in 3 adults in Ireland have been targeted by fraudulent adverts on social media platforms, with Facebook and Instagram being the most identified platforms, followed by X, TikTok and Snapchat.[273] At a broader level, research from Gen estimates that 1 in 3 ads running on Facebook and Instagram in the EU and UK led to a scam,

[267] Interview 4; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[268] Interview 5.

[269] ibid.

[270] Verbraucherzentrale Bundesverband, Jeder zweite Fakeshop schaltet Werbung auf Google oder Meta (2025), available at: https://www.vzbv.de/pressemitteilungen/jeder-zweite-fakeshop-schaltet-werbung-auf-google-oder-meta.

[271] Watchlist Internet, Promis als Lockvögel: Werbung für betrügerische Investmentplattformen erreicht täglich 200.000 Österreicher:innen (2024), available at: https://www.watchlist-internet.at/news/werbung-promis-investmentbetrug/.

[272] ibid.

[273] RTE, One third of social media users targeted by fake adverts (2024), available at: https://www.rte.ie/news/business/2024/1115/1481149-one-third-of-social-media-users-targeted-by-fake-adverts/.

phishing or malware link – of the 14.5 million ads analysed over 23 days, 30.99% of them were fraudulent, gaining more than 300 million ad impressions.[274]

Scammers exploit several technical and procedural features of the advertising systems provided by VLOP and VLOSEs, as detailed in the following paragraphs.

Identity verification: When placing an ad, the advertiser (operating either from a personal account or a business account) may be required by the platform to declare their identity. As per the publicly available 2025 Risk Assessment Reports, this mechanism is present on AliExpress, Amazon, Bing, Facebook, Google's designated services (not implemented for all advertiser accounts yet, as the feature is gradually rolled out), Instagram, and Pinterest (only in relation to shopping ads).[275]

However, it is reported that the designated services mainly rely on **self-declaration as a form of identity verification,** without requesting identity documents or corroborating the data provided against credit card transactions used to pay for the ad.[276] Interviewees reported that scammers often fill in the fields requesting information on the advertiser's identity with **non-pertinent data**, such as random letters or numbers, as no genuine identity verification is required to purchase advertising space.[277]

As part of the stakeholder consultation, one interviewee stated that **scammers can easily create new accounts and new pages to place the same ads** if their account is removed.[278] This finding is corroborated by a study from ÖIAT, which observed that upon removal by Facebook or Instagram of a page running ads for a fake webshop, nine other variations of it appeared, spreading similar ads linking to the same fake webshop.[279] It is important to note that verification does not pre-empt scammers from posting fraudulent ads – stakeholders highlighted instances in which scam ads were posted by verified advertiser accounts.[280]

Similar concerns related to self-declared identities are highlighted by other stakeholders. An investigation from Wien Arbeiterkammer and ÖIAT found that, on TikTok, content (videos and ads) available on the platform can be boosted in their reach by entities other than the original creator/account holder.[281] This function, which allows users to pay for targeted advertising campaigns for third-party content, does not require any means of identification, with the

[274] Gen Digital, The Scam Ad Machine (2026), available at: https://www.gendigital.com/blog/insights/research/scam-ad-machine-meta.

[275] AliExpress, Bing, Facebook, Instagram, Google, Pinterest 2025 Systemic Risk Assessment Reports.

[276] Interviews 5, 6, 9; corroborated by AI Forensics Meta Ads: A Pill Hard to Swallow (2024), available at: https://aiforensics.org/uploads/meta_health.pdf; AI Forensics, TikTok's Research API: Problems without Explanations (2025), available at: https://arxiv.org/pdf/2506.09746.

[277] Interviews 5, 9, 14.

[278] Interview 6; Multi-stakeholder Workshop on Online Financial Scams.

[279] ÖIAT, Numerous fraudulent ghost stores on Facebook and Instagram (2025), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Ghost_Stores_Erhebung_en.pdf.

[280] Multi-stakeholder Workshop on Online Financial Scams.

[281] AK Wien and ÖIAT, #KEINEWERBUNG? Schleichwerbung und problematische Marketingkommunikation auf TikTok (2025), available at: https://wien.arbeiterkammer.at/beratung/konsumentenschutz/achtungfalle/Schleichwerbung_auf_Tiktok_202505.pdf.

maximum amount that can be spent on promoting a single video reportedly being EUR 50,847.45.[282]

One interviewee indicated that bad actors can operate fraudulent advertiser identities and then abandon the accounts once flagged or banned, readily replacing them with new ones, because account creation would carry negligible costs or scrutiny.[283]

Ad review: Generally, ads placed on VLOPs and VLOSEs undergo a review process before becoming available online. Based on the reports and policies published by the designated service providers, this review process first relies on automated moderation, with human reviewer input where nuanced determination is required. These processes are described in depth in Sections 5.1 and 5.2.

In an interview, one stakeholder suggested that scammers may circumvent the ad moderation processes of platforms by **initially submitting legitimate content for review, then switching the content to fraudulent material** once the ad has been verified and placed online.[284] Platforms' ad management systems typically allow editing an ad that was already posted, verified, and approved. Facebook, Instagram and Snapchat, for instance, mention that editing certain details may trigger re-review of the ad, without specifying which details exactly.[285] Meanwhile, TikTok explains that any changes relating to the block list, targeting (including age, location, and language), video, image, display name, URL link, deeplink, profile image, and tracking will lead to the ad being reviewed again.[286]

Beyond this tactic, one investigation claims that scammers also exploit the shortcomings of automated moderation processes by rendering the content more difficult for a machine to read, breaking keyword matching and reducing classifier reliability.[287] The investigation found that, when placing an ad, scammers use **obfuscated characters**, replacing standard letters with similar-looking characters from other alphabets or emojis. These characters look normal to users, but they appear as a different string to the machine, hence avoiding detection.[288] This technique is reportedly also used for **hidden impersonation**, whereby scammers include special spacing characters or joiners which render a person's name visually identifiable by a normal user, but as a different token to the detection system.[289]

Moreover, the same investigation reports that scammers also exploit superficial reviewing processes through **typosquatting**, a technique entailing the registration of destination domain

[282] ibid.

[283] Interview 9.

[284] Interview 5.

[285] Meta, How to edit Facebook and Instagram campaigns in Meta Ads Manager, available at: https://www.facebook.com/business/help/2169779963333459?id=649869995454285; Snapchat, How to Edit an Ad After It's Been Reviewed, available at: https://businesshelp.snapchat.com/s/article/edit-ad-review?language=en_US

[286] TikTok, Changes that Trigger the Review Process, available at: https://ads.tiktok.com/help/article/changes-trigger-review-process

[287] Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll.

[288] ibid.

[289] ibid.

names that closely resemble legitimate brands, with minor differences (spelling mistakes, similar characters, or use of different alphabets).[290] This is coupled with mismatched visual previews for the ad and its actual content – while a video thumbnail may show a legitimate product, the ad's underlying content promotes a scam, going undetected if the automated system or human reviewer does not expand the media or review its whole content.[291]

Several stakeholders claimed there are significant weaknesses in ad content moderation, including the re-checking of advertisers only after specific signals rather than at regular intervals, an absence of quality assurance, user complaints that do not trigger escalation, uneven language moderation, template responses showing no evidence of human intervention, reported internal limits on moderation intervention, and review-speed pressures that generate false negatives.[292]

On the platform side, specifically in relation to Facebook and Instagram, a Reuters investigation claims that Meta would, allegedly, only ban advertisers if its automated ad review system flags them as at least 95% certain to be committing fraud, and in cases of less certainty, the company would charge them a higher ad rate, as a penalty.[293]

Dynamic ads: This is a feature that allows advertisers to run **multiple versions of the same campaign simultaneously**. According to two stakeholder interviews, it appears that scammers use it to embed **a small number of fraudulent ads within a larger set of legitimate ads, seeking to avoid detection**.[294] This finding is corroborated by research from Gen, which found that multi-facet ads, which bundle different images, products, or links into one, are used to combine legitimate destinations with a single malicious or scam-related link, thus lowering suspicion for the reviewing process and for the users.[295] Another study reports that the legitimate ads function as auxiliary cloaking materials, masking fraudulent content and flooding automated detection mechanisms.[296] The bundling of legitimate ads with fraudulent content dilutes the abuse signals registered by the detection system, lowering the chance of it being flagged for review.[297] This dynamic-bundling technique was found to operate at industrial scale rather than as isolated incidents: large volumes of these campaigns were identified running simultaneously from different advertisers, often linked to newly created advertisers and low-history accounts.[298]

---

[290] Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll.

[291] ibid.

[292] Multi-stakeholder Workshop on Online Financial Scams.

[293] Reuters, Meta is earning a fortune on a deluge of fraudulent ads, documents show (2025), available at: https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

[294] Interviews 5, 6.

[295] Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll.

[296] Ewelina Bartuzi-Trokielewicz and Alicja Martinek, Anatomy of Generative Scam Campaigns in Online Advertising Ecosystems (2026), available at: https://dl.acm.org/doi/pdf/10.1145/3774905.3794690.

[297] ibid.

[298] ibid.

URL cloaking: Advertisers are given the option to display **a URL to users that differs from the actual destination to which they will be redirected**. Scammers reportedly use this to display links to legitimate websites while leading victims to scam webpages.[299] A report from Gen suggests that Meta's API surfaces the domain shown in the ad, not necessarily the destination the user reaches after clicking; this renders large-scale, programmatic detection by third parties (i.e., researchers, law enforcement) more difficult.[300]

Separate research from Bitdefender documents a hybridisation of the use of dynamic ads (described above) and hidden links, in which scammers **distribute an ad in multiple versions that share a common dynamic ad URL parameter but differ in destination**.[301] Some ad variants redirect users to clean URLs while others redirect to scam infrastructure such as cloned websites or fraudulent online shops, and Bitdefender found that many of the ads analysed displayed trusted preview domains but redirected users to scam infrastructure once live.[302]

Pages impersonating public figures: Scammers often **use the name and likeness of public figures** to create advertiser pages, publishing advertisements from these impostor accounts. These ads employ video or audio deepfakes of the impersonated entities, further entertaining the illusion of a legitimate endorsement.[303] While this behaviour is prohibited by the platforms' policies, its continued presence in the online environment, as observed by AI Forensics in their research on Instagram and Facebook, is considered by the authors of that report as a potential indication of a sustained failure to detect and remove such content.[304]

Advertising on online search engines: Scammers use paid search advertising to boost the position of fraudulent sites in the list of search results. Through paid ad placements, fraudsters can **position spoofed or cloned websites at the top of the search engine results** pages for relevant queries.[305] In this context, researchers identified Google Ads as a key channel, whereby fraudsters purchase sponsored placements targeting users searching for simple, legitimate services and exploit the prominent positioning and 'Sponsored' label of paid search results to create the illusion of trustworthiness.[306] For example, in relation to subscription scams, a 2026 study by ÖIAT found that 43% of flagged subscription scam domains were

---

[299] AI Forensics Meta Ads: A Pill Hard to Swallow (2024), available at: https://aiforensics.org/uploads/meta_health.pdf.

[300] Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll.

[301] Bitdefender, Global Scam Machines: Inside a Meta-Powered Investment Fraud Ecosystem Spanning 25 Countries (2026), available at: https://www.bitdefender.com/en-us/blog/labs/global-investment-scam-network-using-meta-ads;

[302] ibid.

[303] AI Forensics Meta Ads: A Pill Hard to Swallow (2024), available at: https://aiforensics.org/uploads/meta_health.pdf.

[304] ibid.

[305] ÖIAT, Verbreitung von Abo-Fallen durch Google Ads (2026), available at: https://www.watchlist-internet.at/fileadmin/files/Abo-Fallen/Google-Policy-Paper.pdf; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[306] ÖIAT, Verbreitung von Abo-Fallen durch Google Ads (2026), available at: https://www.watchlist-internet.at/fileadmin/files/Abo-Fallen/Google-Policy-Paper.pdf.

actively advertised on Google's designated services, with 34 problematic advertisers serving nearly 28,000 ads to Austrian users in less than a year alone.[307]

In addition to these feature-specific points, a broader, structural concern has been identified as part of the desk research and stakeholder consultation in relation to the **incentives of VLOPs and VLOSEs providers in relation to the ads that are placed on their services**. Reuters claims that Ad placements represent a significant source of revenue for service providers, with leaked Meta documents alleging that the company earned 10% of its overall annual revenue (USD 16 billion) in 2024 from advertisements for scams and banned goods.[308] As per the investigative journalists, the same documents also highlight that Meta has placed restrictions on the revenue value that may be lost due to vetting questionable advertisers, with content moderation teams allegedly being prohibited from taking ad moderation actions that could cost Meta more than 0.15% of the company's total revenue.[309]

Similarly, a separate investigation by the Wall Street Journal, based on internal Meta documents, alleges that the company has decided not to implement advertiser verification requirements similar to those it mandates for political ads, due to concerns related to loss of revenue from advertisers unwilling or unable to pass identity checks.[310]

The perspective of the journalists at Reuters and at the Wall Street Journal was also shared by stakeholders. Participants in the workshop indicated that platforms have limited incentives to combat scam advertising because they derive revenue from it, describing a structural conflict of interest between monetisation and user protection.[311] To support their claims, these stakeholders referred to the two journalistic investigations above, in addition to parallel research from Gen Digital, which alleges that a significant share of Meta's revenue derives from scam ads, with as many as 30% of its ads considered to be scams.[312] These claims could not be independently verified by the study team.

Researchers and interviewees believe that these financial incentives would translate into limited proactivity; these stakeholders claim that VLOPs and VLOSEs only remove a single ad upon detection or due to external reporting, without identifying its identical copies (which may even be placed by the same advertiser) and taking actions against them.[313] Stakeholders

[307] ibid.

[308] Reuters, Meta is earning a fortune on a deluge of fraudulent ads, documents show (2025), available at: https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

[309] ibid.

[310] The Wall Street Journal, Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook (2025), available at: https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8.

[311] Multi-stakeholder Workshop on Online Financial Scams.

[312] The Wall Street Journal, Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook (2025), available at: https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8; Reuters, Meta is earning a fortune on a deluge of fraudulent ads, documents show (2025), available at: https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/; Gen Digital, The Scam Ad Machine (2026), available at: https://www.gendigital.com/blog/insights/research/scam-ad-machine-meta.

[313] Interviews 5, 6, 9; corroborated by Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll; Watchlist Internet, Massenhaft irreführende Werbung von problematischen Online-Shops auf Facebook und Instagram (2025),

observe that due to this lack of proactive ad moderation, many duplicate fraudulent ads remain publicly accessible to users.[314]

Recommender systems

Recommender systems are normally algorithmic systems used by online platforms to suggest content based on personalisation or other criteria, usually seeking to maximise engagement. They also allow platforms to gain behavioural insight into the users. These systems are considered by some researchers to face a range of ethical challenges due to one of their objectives being to maximise engagement and user retention, which can be achieved by surfacing sensationalist, attention-grabbing content that may in fact be illegal or harmful.[315] Content visibility is often based on user engagement metrics and algorithmic decisions; these mechanisms do not in themselves a priori distinguish between legitimate and harmful information, their primary aim being to surface content that keeps the audience engaged.[316]

At the user level, scholars argue that recommender systems function as a hybrid between content-based recommendations and collaborative filtering. Content-based recommendations are fuelled by the general popularity of content among users: popular content is recommended to more users, becoming even more popular.[317] Collaborative filtering is based on the values and interests assigned to that content by groups of users with similar profiles and interests: content is recommended because similar users have engaged with it.[318] The recommender system of each platform is theorised to function across these two axes, dynamically shifting the weight from one approach towards the other, based on the user's response.[319] By applying this theoretical model to **online scam content**, it can be posited that this type of content is **surfaced in users' feeds either due to general popularity or due to the users' affinities or interests in specific topics or sub-groups**. Examples of the latter can be observed in

available at: https://www.watchlist-internet.at/news/irrefuehrende-werbung-auf-meta-plattformen/?sword_list%5B0%5D=werbung&no_cache=1; EDMO, Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU (2025), available at: https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.

[314] ibid.

[315] eSafety Commissioner Australia, Position statement – Recommender systems and algorithms (2023), available at: https://www.esafety.gov.au/industry/tech-trends-and-challenges/recommender-systems-and-algorithms/full-position-statement.

[316] Massimo Terenzi, Modelling Persuasion in Social Media: A Theoretical Approach to Algorithmic Content Distribution and Manipulation (2024), available at: https://papiro.unizar.es/ojs/index.php/rc51-jos/en/article/view/10992.

[317] ibid; Jesus Bobadilla et al., Recommender systems survey (2013), available at: https://romisatriawahono.net/lecture/rm/survey/information%20retrieval/Bobadilla%20-%20Recommender%20Systems%20-%202013.pdf; Engin Bozdag, Bias in algorithmic filtering and personalization (2013), available at: https://www.researchgate.net/publication/257560404_Bias_in_algorithmic_filtering_and_personalization.

[318] Massimo Terenzi, Modelling Persuasion in Social Media: A Theoretical Approach to Algorithmic Content Distribution and Manipulation (2024), available at: https://papiro.unizar.es/ojs/index.php/rc51-jos/en/article/view/10992; Zeynep Batmaz et al., A review of deep learning for recommender systems: challenges and remedies (2018), available at: https://daiwk.github.io/assets/Batmaz2018_Article_AReviewOnDeepLearningForRecomm.pdf.

[319] ibid.

relation to investment scams or health scams, where the victim has previously engaged with similar content (even potentially legitimate).[320]

As noted by the UK Parliament, it is difficult to establish clear causal links between the inherent functioning of recommender systems and harm, due to limited transparency into the functioning of the algorithms.[321] The research conducted as part of this study points to a similar data gap on the relation between recommender systems and online financial scam content. However, this relation can be influenced by external actors (scammers), who exploit the functioning of the algorithms to amplify their fraudulent content.

The objective of this manipulation is to maximise reach and exposure to scam content. One research paper suggests that prolonged or repeated exposure to highly engaging content promoting scams (e.g., investment narratives, exclusive offers) can normalise implausible claims, gradually directing users from relatively benign content towards increasingly risky or fraudulent environments.[322]

Multiple means to manipulate the recommender algorithms of online platforms are identified in the literature and by stakeholders. For example, through **coordinated inauthentic behaviour attacks**, scammers share the same content in very short time intervals from different accounts, tricking the algorithm into conflating this upsurge in traction with relevance or veracity, and further promoting it to other users.[323] This leads to a feedback loop, whereby the reach of the scam content is amplified even further, as more and more legitimate users organically engage with it.

Stakeholders consulted as part of this study have also noted that scammers **adapt the promotion and content of their scams to match current trends, with a view to maximising the reach of their posts**.[324] They alledgedly test the visibility and success rates of their content, identifying the types of posts that reach the highest audience and entrap the most victims.[325] Viral trends and current events are deliberately incorporated into scam content to generate engagement on social media, with scam narratives adapted to what is most likely

[320] Jingjia Xiao, Qing Xiao and Hong Shen, “It felt real” victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680; Hongliang Chen, et al., Examining older adults’ vulnerability to online health scams: insights from routine activity theory (2025), available at: https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2025.1585851/full.

[321] UK Parliament – Science, Innovation and Technology Committee, Social media, misinformation and harmful algorithms (2025), available at: https://committees.parliament.uk/publications/48745/documents/258221/default/.

[322] Jingjia Xiao, Qing Xiao and Hong Shen, “It felt real” victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[323] Massimo Terenzi, Modelling Persuasion in Social Media: A Theoretical Approach to Algorithmic Content Distribution and Manipulation (2024), available at: https://papiro.unizar.es/ojs/index.php/rc51-jos/en/article/view/10992; Fabio Gigglietto et al., Coordinated Link Sharing Behavior as a Signal to Surface Sources of Problematic Information on Facebook (2020), available at: https://dl.acm.org/doi/10.1145/3400806.3400817.

[324] Interviews 1, 4; Multi-stakeholder Workshop on Online Financial Scams.

[325] Multi-stakeholder Workshop on Financial Scams.

to capture users' attention at a given moment.[326] Scammers also rely on the use of clickbait headlines or emotional triggers to increase the visibility of misleading content.[327]

In one interview, one stakeholder gave the example of how scammers quickly capitalised on the rising popularity of Punch the Monkey.[328] The small monkey became viral online due to its attachment to a stuffed toy that replaced the monkey's mother, who had abandoned it. Scammers used its likeness to organise fraudulent charity or donation scams.[329] On a broader level, scammers adapted their narrative to current geopolitical events, such as the COVID-19 pandemic, the humanitarian situation in Ukraine or Gaza, or the earthquakes in Türkiye.

A specific phenomenon is observed on marketplaces, where scammers make use of **fake reviews to manipulate the recommendation algorithms and to promote their products** – this process is referred to as 'shilling attacks' or 'fake review injections'.[330] Research carried out by the UK Competition and Markets Authority (UK CMA) shows that 89% of consumers use online customer reviews when researching a product or service.[331] Given the importance of reviews in the consumer's decision process, scammers rely on the manufacturing of fake reviews as a means of enhancing the credibility of the scam through 'social proof'.

The fake reviews count towards the 'star' rating of products or places, which translates into positive engagement and further visibility through the recommender system. Research shows that biased early reviews produce persistent distortions in the functioning of the algorithm, even when the fake reviews have been eventually removed.[332] Consumer organisations claim that the increased prevalence of fake reviews points towards a failure to verify the veracity of reviews, and to assess how they are accounted for by the recommender system.[333] Some designated services (Amazon Store, Google Maps and Google Search) have already been

[326] Interviews 1, 4.

[327] Csongor Herke and Barbara Szabo, Artificial Intelligence and Crime on Social Media Platforms (2026), available at: https://www.intechopen.com/online-first/1249383.

[328] Interview 1.

[329] ibid.

[330] Europol, Internet Organised Crime Threat Assessment 2025 (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf; OECD and European Union Intellectual Property Office, Misuse of E-Commerce for Trade in Counterfeits (2021), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/10/misuse-of-e-commerce-for-trade-in-counterfeits_dfd7df43/1c04a64e-en.pdf. https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-027_how_to_make_online_reviews_more_reliable.pdf.

[331] UK CMA, Consumer spending after reading online reviews (2025), available at: https://assets.publishing.service.gov.uk/media/5a809326ed915d74e33fb346/Infographic_on_consumer_spending_after_reading_online_reviews.PDF.

[332] Panagiotis Adamopoulos, The Spillover Effect of Fraudulent Reviews on Product Recommendations (2024), available at: https://dl.acm.org/doi/10.1287/mnsc.2021.02612; Tommaso Bondi, Michelangelo Rossi, Online Reviews: Information Content, Drivers, and Platform (2026), available at: https://www.ifo.de/DocDL/cesifo1_wp12427.pdf;

[333] BEUC, Turning Stars into Trust: How to make online reviews more reliable (2025), available at: https://www.beuc.eu/position-paper/turning-stars-trust-how-make-online-reviews-more-reliable.

the subject of investigation in this regard, leading to them signing undertakings committing to enhance their systems for tackling fake reviews before the UK CMA.[334]

Artificial streaming scams represent a specific phenomenon that directly targets the functioning of recommender systems, with a view to manipulating them. By using artificially generated engagement (views, likes, comments), it was found that scammers generate a false impression of popularity, thus reaching monetisation, increasing ranking in search or recommender results, and gaining even more (authentic) viewership.[335] This type of scam directly exemplifies how recommender systems can be gamed for financial gain by malicious perpetrators.

Organic content and content moderation

Designated services offer a range of content creation functionalities that scammers exploit to perpetrate online financial scams. This section examines these functionalities, focusing on the role played by organic content in facilitating the dissemination and perceived legitimacy of scam content.

'Organic content' is understood as user-generated material, including profiles, posts, comments, stories and live broadcasts, that circulates through ordinary platform mechanisms, rather than through paid promotion or sponsored placement.

Scam content is often difficult to distinguish, in form and presentation, from material produced by legitimate users. Researchers posit that classic **social engineering techniques are especially effective on online platforms** (particularly social media) because users are presented with cues that mimic genuine relationships and brands (profile pictures, follower counts, comments), which serve as heuristic shortcuts for credibility.[336] As such, organic content inherently carries a baseline level of perceived credibility, rendering it a particularly effective vector for fraudulent schemes.

Firstly, scammers abuse account creation functions to build **fake profiles**. This is facilitated by the shortcomings of identity verification mechanisms, which primarily rely on self-declaration of personal information (as also described above in relation to ad placements).[337] In an interview, one stakeholder stated that scammers often set up online profiles using false, stolen or intentionally inaccurate information.[338] By misrepresenting their age, gender,

[334] UK CMA, UNDERTAKING TO THE COMPETITION AND MARKETS AUTHORITY ('CMA') PURSUANT TO SECTION 219, PART 8, ENTERPRISE ACT 2002 ('EA02') RELATING TO THE CONSUMER PROTECTION FROM UNFAIR TRADING REGULATIONS 2008 ('CPRs') (2025), available at: https://assets.publishing.service.gov.uk/media/6841a7ca578282a4b102c0ab/Amazon_s_undertaking_to_the_CMA_.pdf; UK CMA, UNDERTAKING TO THE COMPETITION AND MARKETS AUTHORITY ('CMA') PURSUANT TO SECTION 219, PART 8, ENTERPRISE ACT 2002 ('EA02') RELATING TO THE CONSUMER PROTECTION FROM UNFAIR TRADING REGULATION (2025), available at: https://assets.publishing.service.gov.uk/media/67924902e982ca138427fc1e/Google_s_undertaking_to_the_CMA.pdf

[335] Andrew Chu et al., Behind the Tube: Exploitative Monetization of Content on YouTube (2022), available at: https://www.usenix.org/system/files/sec22-chu.pdf/

[336] Csongor Herke and Barbara Szabo, Artificial Intelligence and Crime on Social Media Platforms (2026), available at: https://www.intechopen.com/online-first/1249383.

[337] Interview 2; see also Finans Danmark, Styrket bekæmpelse af digital svindel - Svindel Task Forcens 18 anbefalinger (2024), available at: https://www.ft.dk/samling/20241/almdel/ERU/bilag/81/2948819/index.htm.

[338] ibid.

appearance, location, or other personal information, scammers seek to create a false sense of security.[339] For example, fake profiles impersonating friends or peers of a similar age are common in the context of financial scams targeting minors and young adults.[340] While the anonymity afforded by fake profiles is leveraged across all types of financial scams identified, it plays a particularly important role in long-running scams, such as traditional romance scams, sextortion or romance baiting, as it allows scammers to maintain prolonged contact with victims and to build a relationship of trust.[341] Similarly, fake profiles play an important role in rental scams, as perpetrators impersonate real hosts and landlords, often stealing photographs and details from legitimate listings to construct convincing profiles. Another instance is in fake job scams, as false 'recruiter' profiles are created to reach out to victims, or in event ticket scams.[342]

Scammers may then rely on content creation or engagement functions on social media, such as **posts, stories, comments or live broadcasts.** Survey respondents from eight Member States identified direct messages, comments under posts, and replies to stories as frequent initial contact methods.[343] For example, comments under posts or posts in groups can be used to attract victims as part of event ticket scams.[344] Fake comments are also reportedly used to provide 'social proof' to the scam, with other 'scam-users' leaving positive reviews as to the benefits or earnings they incurred, particularly in the context of investment scams.[345]

Stories or live broadcasts on social media platforms have also been reported as being used for the sale of fraudulent health and wellness goods or counterfeits.[346] These channels allow sellers to promote illicit products on a temporary basis, thereby **limiting the traceability** of their actions as soon as the stories expire or the live broadcast sessions end.[347] In addition to ephemeral content, there have also been accounts of regular social media posts being used

[339] Arezou Behfar et al., A First Look into Fake Profiles on Social Media through the Lens of Victim's Experiences (2024), available at: https://dl.acm.org/doi/pdf/10.1145/3678884.3681889.

[340] ibid; Thorn, Trends in Financial Sextortion (2024), available at: https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf;

[341] Rasha Kassem and Elisabeth Carter, Mapping romance fraud research – a systematic review (2024), available at: https://www.emerald.com/jfc/article-abstract/31/4/974/1238258/Mapping-romance-fraud-research-a-systematic-review?redirectedFrom=fulltext.

[342] Sophie Van Der Zee et al., The gift of the gab: Are rental scammers skilled at the art of persuasion? (2019), available at: https://arxiv.org/abs/1911.08253; Vice, Scammers Are Sending Fake Job Offers on LinkedIn (2021), available at: https://www.vice.com/en/article/scammers-are-sending-fake-job-offers-on-linkedin/; Take Five, Ticket scams, available at: https://www.takefive-stopfraud.org.uk/protect-yourself/ticket-scams/.

[343] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[344] Take Five, Ticket scams, available at: https://www.takefive-stopfraud.org.uk/protect-yourself/ticket-scams/.

[345] Demagog, Metoda „na walizkę" – jak działają oszuści na Facebooku? (2024), available at: https://demagog.org.pl/analizy_i_raporty/jak-oszusci-z-cypru-okradaja-polakow-oto-historia-pani-iwony/.

[346] Union des Fabricants (UNIFAB), Counterfeiting & Organised Crime (2025), available at: https://www.unifab.com/wp-content/uploads/2025/06/UNIFAB_Contrefacon-Criminalite_ENGLISH_VDEF_03062025.pdf.

[347] ibid.

to promote scams, particularly insurance scams.[348] A notable form of organic content relevant to the dissemination of online scams involves the use of so-called 'finfluencers' for investment scams – this topic is explored in depth as part of case study A, under Section 6.1.

The content available to users online may also hinder their ability to discern scam content from legitimate, harmless posts. Increasingly, researchers point towards the increasing presence of **low-quality, mass-produced synthetic content** (popularly referred to as 'AI slop') which **floods users' feeds**.[349] A novel strand of literature hypothesises that this **pollution of the digital information ecosystem blurs the boundaries between false and legitimate content**, undermining the epistemic foundations of online discourse and rendering it increasingly difficult for users to identify what is harmful.[350] In the fast-paced environment of online media, **repeated exposure to and consumption of low-quality 'slop' content** is theorised to desensitise the user, lowering their propensity to question or critically engage with the content they consume.[351] This **leaves users more vulnerable to scam content**, which is hidden between other low-quality posts that prime the user for gullibility.

Overall, the widespread presence of scam content on online platforms has given rise to questions from stakeholders as to the content moderation efforts of the designated services, and their results.[352] A concern mentioned during the stakeholder consultation refers to the speed with which platforms react to reports submitted by users and by trusted flaggers, and the moderation decisions taken in response - multiple interviewees have expressed doubts as to the effectiveness of the reporting feature, arguing that, in their experience, platforms rarely act upon user reports, with even fewer instances of positive outcomes.[353] These concerns are explored in more detail in Section 5.3.

Monetisation systems

Another risk factor identified by the stakeholders interviewed relates to platform monetisation systems.[354] It was indicated that **revenue redistribution programmes on social media platforms create incentives for the creation of high-volume, engagement-maximising content, which can overlap with or transition into fraudulent behaviour**.[355] This

[348] Insurance Europe, Insurance Europe response to EC consultation on online fraud (2026), available at: https://www.insuranceeurope.eu/mediaitem/c356079f-c353-4754-a049-1a0054e0b29b/Insurance+Europe+response+to+EC+consultation+on+online+fraud.pdf?inline=1.

[349] AI Forensics, AI-generated Algorithmic Virality (2025), available at: https://aiforensics.org/uploads/GenAI%20Report.pdf.

[350] Giada Marino et al., Exploring the Zombie Internet: Anatomy of Three Deceptive Information Operations on Facebook (2026), available at: https://rosa.uniroma1.it/rosa03/mediascapes/article/view/19402; Prathamesh Muzumdar et al., The Dead Internet Theory: A Survey on Artificial Interactions and the Future of Social Media (2025), available at: https://arxiv.org/abs/2502.00007.

[351] William X.Q. Ngiam et al., "Endless Mind-Numbing Slop": A Qualitative Analysis of the Perceived Impact of Digital Technology on Attention (2026), available at: https://online.ucpress.edu/collabra/article/12/1/161934/218241/Endless-Mind-Numbing-Slop-A-Qualitative-Analysis.

[352] Interviews 6, 7, 8; Multi-stakeholder Workshop on Online Financial Scams.

[353] ibid.

[354] Interview 8; Multi-stakeholder Workshop on Online Financial Scams.

[355] ibid.

perspective is corroborated by What To Fix, which notes that the shift towards performance-based monetisation incentivises content creators to rely on inauthentic and automated uses of service, which can be linked to artificial streaming scams.[356] For instance, an interviewee has indicated concern that individuals operating large networks of inauthentic accounts in Southeast Asia may shift from monetisation-driven content creation to financial scam operations when platform revenue programmes are scaled back.[357]

In addition to inauthentic content (that may include scam content), platform monetisation systems may also incentivise content creators to produce or participate in scams, as noted by the European Board for Digital Services Report.[358] Examples of this phenomenon include 'influencers benefitting from affiliate programmes and engagement-based payouts when disseminating authentic, but harmful content such as scams'.[359] The literature calls for more research on the actors that profit from the proliferation of deceptive content, including online scams, on social media.[360] For that reason, the understanding of monetisation systems as risk vectors for online scams remains hypothetical, with additional research needed to establish under what circumstances such financial incentives may influence content creators to engage in scams.

Search engine results

Search engine results represent another important dissemination vector for online financial scams, primarily identified in relation to investment scams, undelivered products or counterfeit scams, insurance scams, loan or credit offer scams, or charity and disaster relief scams. Beyond search engine ad placements (described above), the literature suggests that **scammers also manipulate search engine results to surface fraudulent pages to users searching for genuine queries**, as described below.

To understand how scammers exploit search engines, it is important to briefly describe the functioning of this type of service. A search engine performs three broad functions: crawling, indexing and ranking. Automated programs ('crawlers') traverse the web by following links from page to page, discovering new and updated content. Once a page is crawled, the search engine parses its content - text, headings, images, structured data (schema markup), and metadata - and stores a processed representation of it in a database ('the index'). When a user submits a query, the engine searches the index, then runs a ranking algorithm to order matching results by predicted relevance and quality.

[356] What To Fix, Systemic Risks – Social Media Monetization Systems: A Risk Factor (2025), available at: https://drive.google.com/file/d/1UeKYU3qyeOfEY--oz2hovSpAtx-upOoD/view.

[357] Interview 8, corroborated by UN Office on Drugs and Crime, Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia (2025), available at: https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.

[358] European Board for Digital Services, Second Report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risk as well as mitigation measures (2026), available at: https://digital-strategy.ec.europa.eu/en/library/second-report-systemic-risks-very-large-online-platforms-and-search-engines-under-digital-services.

[359] ibid.

[360] Carlos Diaz Ruiz, Disinformation on digital media platforms: A market-shaping approach (2025), available at: https://journals.sagepub.com/doi/pdf/10.1177/14614448231207644; see also sources cited therein.

Scammers rely on a range of techniques, which are commonly referred to as Search Engine Optimisation (SEO) poisoning or black-hat SEO, to manipulate the functioning of the search engine's algorithms.

One technique involves **installing malicious code (malware)** on compromised websites to intercept server requests and return fabricated content, causing search engines to index fraudulently generated pages as if they formed part of established legitimate sites, to achieve high search rankings for fraudulent stores.[361] This type of technique directly targets the functioning of crawling and indexing algorithms.

A related technique targets previously **legitimate, expired domain names** that still carry strong search rankings and backlink profiles, repurposing them for fraudulent content so the new, malicious site inherits the organic authority of the domain.[362] Similarly, this technique also targets the functioning of indexing algorithms.

An approach that is becoming more prevalent is **cloaking**, whereby different content is served to different user segments: a cloaker will serve 'benign' content to search engine crawlers and scam content to normal visitors who access the website through a search result.[363] This circumvents the ability of the search engine algorithms to detect fraudulent websites.

Scammers can also manipulate or exploit the functioning of ranking algorithms by **cramming irrelevant keywords into the website to mislead the algorithm ('keyword stuffing') or by artificially increasing a website's click-through rate ('link farms')**, using bots or humans for fake clicks, to boost the perceived popularity of the destination.[364] They also generally monitor trends in search queries, deploying scam websites that include high-traffic keywords that users are likely to look for – to that end, cybersecurity firms warn that AI systems will soon be able to monitor trending search queries in real time and automatically generate and optimise malicious content for search rankings without human intervention, potentially allowing a single actor to poison results for thousands of keywords simultaneously.[365]

Some researchers argue that this manipulation of search engine results is also facilitated by search engines themselves, with **a recent longitudinal study reporting that the accuracy of search results from Google Search has decreased by approximately 10% compared to previous years,** and that higher-ranking pages are 'more optimised, more monetised with affiliate marketing, and show signs of lower text quality'.[366] Moreover, the study also found an

[361] Makoto Shimamura, Uncovering Black-hat SEO based fake E-commerce scam groups from their redirectors and websites (2025), available at: https://arxiv.org/html/2505.21021v1

[362] Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar.

[363] Interview 5; Multi-stakeholder Workshop on Online Financial Scams; see also David Y Wang et al., Cloak and Dagger: Dynamics of Web Search Cloaking (2011), available at: https://dl.acm.org/doi/pdf/10.1145/2046707.2046763.

[364] Crowdstrike, What is SEO poisoning? (2023), available at: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/seo-poisoning/.

[365] VectraAI, SEO Poisoning Attacks: How Cybercriminals Weaponize Search Results (2025), available at: https://www.vectra.ai/topics/seo-poisoning.

[366] Janek Bevendorff et al., Is Google Getting Worse? A Longitudinal Investigation of SEO Spam in Search Engines (2024), available at: https://downloads.webis.de/publications/papers/bevendorff_2024a.pdf.

increasing trend towards simplified, repetitive, and potentially AI-generated content.[367] While Google has publicly assumed commitments to reduce the amount of low-quality content on Search, the researchers claim that the improvements have a temporary effect, with SEO manipulators finding new ways to bypass the systems.[368] This strand of research is, however, still developing, with limited longitudinal data to corroborate this conclusion – therefore, this hypothesis remains to be further tested.

App store content

A phenomenon less documented relates to the use of application stores by fraudsters to make fake investment applications available to victims across different countries and in multiple languages. This phenomenon has been primarily observed by Europol in relation to investment scams (both traditional and crypto-based ones).[369] These false investment apps often impersonate legitimate financial institutions or offer fake high-yield trading opportunities, sometimes showing fake profits to encourage further, larger deposits before locking users out.[370]

Scammers may evade the scrutiny of app store review processes by **disguising malicious apps as benign 'Mask Apps'; these are malicious apps that activate hidden functionalities after they are downloaded or when the user interacts with them in a specific manner**.[371] These apps generally display innocent-looking interfaces and limited functionalities, designed to quickly pass the review processes of app stores.[372] These apps include a concealed activation mechanism, which is used to trigger their functionalities – upon activation, the app generally presents a new user interface and functions.

An investigation from Group-IB identified such a fraudulent application on the Apple AppStore, which remained available for download for several weeks before removal.[373] The app, which was masked as a calculator app, collected identification documents, personal information, and banking information, and victims were prompted to fund their account.[374] After a few seemingly successful trades, the victim is persuaded to invest more – however, they soon discover they are unable to withdraw any funds.

The researchers at Group-IB believe that the scammers used a time-based trigger. Before 22 July 2024 at 00:00, the app showed a fake activity screen that showed harmless content,

[367] ibid.

[368] ibid.

[369] Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en.

[370] ibid.

[371] Yijun Zhao et al., No Source Code? No Problem! Demystifying and Detecting Mask Apps in iOS (2024), available at: https://dl.acm.org/doi/pdf/10.1145/3643916.3644419.

[372] Yeonjoon Lee et al, Understanding iOS-based Crowdturfing Through Hidden UI Analysis (2019), available at: https://par.nsf.gov/servlets/purl/10172762.

[373] Group IB, Pig Butchering Alert: Fraudulent Trading App targeted iOS and Android users (2024), available at: https://www.group-ib.com/blog/pig-butchering/.

[374] ibid.

helping it pass Apple's checks. After that date, it could load the fraudulent trading interface, allowing the scam to operate while already being available in the App Store.[375] Similar research identified several illegal gambling apps (linked to gambling scams) on the Apple AppStore, all designed to circumvent the app review process through the deployment of Mask Apps.[376]

Reportedly, fraudsters also circumvent the review processes to which applications are subjected before being placed on app stores by **using bait-and-switch tactics, disguised code or by hijacking the likeness of legitimate apps ('counterfeit apps')**.[377] For example, in April 2026, a fake version of the Ledger Live app (a cryptocurrency wallet app) was made publicly available through the Apple AppStore, leading to losses of approximately USD 9.5 million (EUR 8.126 million).[378] The approval of the fake app is considered by the researchers at AppleInsider to point towards flaws in the comprehensiveness of the app review process, considering that the genuine Ledger Live app already existed on the store, and the fake version had been submitted by an entity (Leva Heal) completely unrelated to the Ledger SAS company.[379]

Private messaging functions

Private messaging functions serve as a critical intermediary step in many online financial scams, enabling fraudsters to move victims away from the relative oversight of public platforms into more private, unmoderated environments where trust can be cultivated and manipulation intensified.[380]

As per the stakeholder consultation, **scammers primarily rely on the private, encrypted nature of the conversation channels provided by messaging services**.[381] However, there is also a trend involving the use of open groups as part of investment frauds, whereby the groups simulate a genuine investor community, with fabricated testimonials and AI-generated member profiles which are used to create the impression of social proof.[382] The German financial regulator BaFin issued approximately one hundred warnings in 2025 concerning suspicious or fraudulent chat groups, the majority of them operating through WhatsApp.[383]

---

[375] Ibid.

[376] Yeonjoon Lee et al, Understanding iOS-based Crowdturfing Through Hidden UI Analysis (2019), available at: https://par.nsf.gov/servlets/purl/10172762.

[377] AppleInsider, App Store scams are getting worse and Apple isn't doing enough (2026), available at: https://appleinsider.com/articles/26/04/17/app-store-scams-are-getting-worse-and-apple-isnt-doing-enough.

[378] AppleInsider, Bogus crypto wallet on App Store steals $9.5M (2026), available at: https://appleinsider.com/articles/26/04/14/bogus-crypto-wallet-on-app-store-steals-95m.

[379] ibid.

[380] Interview 2; It is noted that interpersonal communication services (NIICS) fall outside the substantive scope of the Digital Services Act, in accordance with Recital 14. This function has however been included under this section for comprehensiveness and structural purposes.

[381] Interviews 4, 5.

[382] Interview 5.

[383] Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Investitionen in Kryptowerte und der Einfluss sozialer Medien auf das Anlageverhalten (2026), available at:

Messaging services are used for several distinct purposes within the scam cycle. One interviewee indicated that they **facilitate trust-building** through personalised, one-to-one or small-group interaction, enabling scammers to simulate the kind of individual support that increases victims' confidence in the investment opportunity.[384] They also allow scammers to **evade platform moderation**, with fraudsters relying on environments where end-to-end encryption and the absence of public moderation create what one respondent to the survey described as a 'dark space' for social engineering, largely outside the reach of automated monitoring or regulatory oversight.[385]

Messaging services are also used to coordinate the operational steps of the scam itself: sharing links to fraudulent websites or crypto wallets, sending phishing files, QR codes, or payment instructions, and maintaining real-time contact with victims to counter objections and escalate pressure.[386] According to the survey conducted with national authorities, the role of WhatsApp, in this case used as NIICS, is particularly significant as its wide adoption eliminates the need to prompt victims to install an unfamiliar application.[387] Moreover, it supports media attachments used to transmit fake documents and fabricated investment statements, and it allows video calls through which fraudsters can use deepfake technology to conceal their identity.[388]

Against the background of these findings, the following sections present the perspective of VLOPs and VLOSEs on the risk factors present on their services.

3.1.2. Overview of risk factors identified by designated service providers

The following sections focus on the Systemic Risk Assessment Reports (SRAs) published by the designated services in 2025. The complete list of SRAs with hyperlinks is available in Annex I. For methodological clarity, and to ensure objectivity in the findings of the other sections of this report, these reports have been treated as a separate source of information. This allows the reader to draw their own comparisons as to the landscape of online financial scams, as reported by designated services and by other stakeholders. The countermeasures that designated services report implementing to address these identified risks are analysed separately in Section 5, with detailed platform-by-platform information provided in Annex V.

Across the risk assessments reviewed, financial scam-related risks are articulated through a set of recurring structural risk factors. These do not correspond directly to individual scam typologies, but they instead reflect vulnerabilities in platform design, trust architecture and commercial infrastructure that enable fraudulent practices to emerge and persist at scale.

https://www.bafin.de/DE/Aufsicht/Fokusrisiken/Fokusrisiken_2026/RIF_verbraucher_sozialemedien/RIF_verbraucher_sozialemedien_node.html;jsessionid=7482B626CD4BA5A50D21116827D3E0A2.internet012.

[384] Interview 4.

[385] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[386] ibid, Interview 4.

[387] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[388] ibid.

Inauthentic Identity and Account Manipulation

The manipulation of identity through fake accounts, brand or individual impersonation, the use of bots, and account takeover via stolen credentials are the most consistently identified risk factors across VLOPs and VLOSEs, irrespective of service types. This malicious behaviour is identified in varying degrees of specificity in the 2025 SRAs from TikTok, X, Instagram and Facebook (Meta), LinkedIn, Snapchat, Pinterest, Bing, Google Search, AliExpress and Booking.com.

Designated services consistently frame this as a structural rather than incidental risk, because fake or compromised accounts do not cause harm in isolation, but they serve as enabling infrastructure for a wide range of downstream fraudulent practices, including deceptive advertising, fraudulent listings, scam content in feeds, and direct-message fraud. X explicitly identifies anonymity and broad reach as platform features that can be leveraged to amplify this risk.[389] LinkedIn rates the creation of fake profiles used to approach members privately as one of the primary manifestations of its consumer protection and fraud risk, which it characterises as critical in terms of inherent risk, given the expected probability of occurrence and high severity of potential harm.[390] Pinterest notes that account takeovers, whereby attackers exploit existing accounts rather than creating new ones, represent a distinct variant of this risk, as they allow malicious actors to exploit the trust signals already associated with established accounts.[391] Facebook and Instagram describe prohibitions on identity misrepresentation and artificial content inflation as core pillars of their integrity framework, while noting that generative AI-powered tactics are increasingly used to conduct inauthentic behaviour at scale.[392]

Deceptive Commercial Content - Advertising, Listings and Reviews

A second cluster of risk factors concerns the integrity of commercial information presented to users, spanning advertising systems, product or service listings, and user-generated reviews. Scammers exploit these mechanisms that platforms make available for legitimate commercial communication, thus undermining the informational basis on which users make economic decisions. Platforms' own risk assessments frequently treat them as related or overlapping risk drivers within the consumer protection systemic risk category.

Multiple platforms identify the exploitation of advertising infrastructure to disseminate fraudulent or misleading content as a high-impact risk factor, given the scale and targeting capabilities involved. This risk is identified in the 2025 SRAs from AliExpress, X, TikTok, Snapchat, Instagram and Facebook (Meta), Google Search, YouTube, Google Shopping and Bing. Bing's assessment explicitly notes that advertising fraud has attracted sustained regulatory attention in the preceding year and flags the amplifying effect of generative AI on this risk.[393] Apple App Store notes risks arising from advertising content that violates consumer protection law, while characterising its own advertising infrastructure as presenting a lower risk profile relative to other platform types.[394] Google Shopping identifies unfair commercial

[389] X 2025 Systemic Risk Assessment Report.

[390] LinkedIn 2025 Systemic Risk Assessment Report.

[391] Pinterest 2025 Systemic Risk Assessment Report.

[392] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[393] Bing 2025 Systemic Risk Assessment Report.

[394] Apple AppStore 2025 Systemic Risk Assessment Report.

practices, including scams and inaccurate product representations, as an area of inherent risk.[395]

In relation to product and service listings, the risk of fraudulent, misleading or incomplete commercial information being presented to users is identified primarily by marketplace platforms (Amazon, Zalando, Shein, Booking.com). Amazon centres its consumer protection risk analysis on the risk that its EU Store may be abused to offer illegal, unsafe or counterfeit products.[396] Zalando identifies a granular set of sub-risks relating to incorrect or missing product information, pricing errors and inaccurate seller details, each assessed at low to very low residual risk levels.[397] Shein identifies risks from misleading product content and from seller-generated deceptive information, including potential manipulation of product listings.[398] Booking.com identifies fraudulent property listings, including non-existent properties used to extract payments, as an area in which inherent risk has risen due to more sophisticated AI-driven fraud tools.[399]

Fake, manipulated or AI-generated reviews are identified particularly by marketplace and app-distribution platforms (AliExpress, Amazon, Apple App Store, Zalando, Shein and Google Maps, Google Play and Google Shopping) as mechanisms that distort consumer decision-making and facilitate the commercial success of fraudulent or deceptive offerings. AliExpress explicitly identifies attempts to use AI to generate reviews as an emerging threat.[400] Apple App Store notes the risk of fake ratings being amplified via bots.[401] Google Maps and Play describe monitoring for coordinated campaigns to artificially manipulate listing scores.[402]

Fraudulent Use of Private Communication Channels

Several platforms identify in-platform private messaging environments as a structurally distinct risk domain for financial fraud. The crucial risk dimension of these features lies in the enforcement constraints: once interactions move out of publicly visible spaces and into private messages, the platform's ability to detect and intervene is reduced, and users may be more susceptible to manipulation.

LinkedIn provides the most detailed account of this risk among the platforms reviewed, identifying as specific manifestations the defrauding of members through private messages, including through the sharing of advertising links redirecting users to fraudulent external content or malware.[403] AliExpress, Instagram, Facebook and Snapchat also identify private messaging or off-platform redirection as relevant risk vectors, with the common idea being the

[395] Google 2025 Systemic Risk Assessment Report.

[396] Amazon Store 2025 Systemic Risk Assessment Report.

[397] Zalando 2025 Systemic Risk Assessment Report.

[398] Shein 2025 Systemic Risk Assessment Report.

[399] Booking.com 2025 Systemic Risk Assessment Report.

[400] AliExpress 2025 Systemic Risk Assessment Report.

[401] Apple AppStore 2025 Systemic Risk Assessment Report.

[402] Google 2025 Systemic Risk Assessment Report.

[403] LinkedIn 2025 Systemic Risk Assessment Report.

use of direct communication to initiate or complete fraudulent transactions beyond the reach of content moderation systems.[404]

Illegal and Counterfeit Goods

The offer and promotion of counterfeit or otherwise illegal products is a distinct risk category primarily for large transactional marketplace platforms, where it is captured principally under the illegal content systemic risk rather than solely under fundamental rights. AliExpress, Amazon, Zalando, Shein, Google Search, Google Shopping and TikTok all identify this risk.[405]

The framing used by these platforms varies significantly. Amazon characterises the risk of illegal, unsafe or counterfeit products as endemic to online retail as a whole, pre-dating the platform and not specific to large-scale operators, and explicitly integrates its fundamental rights assessment within its illegal content analysis on the basis that the two are inseparable given its business model.[406] AliExpress similarly contextualises its consumer protection risk by reference to evidence from peer marketplaces and independent regulatory findings, framing it as a sector-wide challenge.[407] Zalando maps a highly granular set of sub-risks relating to product labelling, certification requirements and information accuracy.[408]

AI as an amplifier of online financial scams

Cutting across all platform types is the growing role of AI, acknowledged by a subset of platforms (AliExpress, Facebook, Instagram, Booking.com, Bing, Apple App Store) as an amplifier or influencing factor of existing scam risks rather than a source of qualitatively new ones.[409] Generative AI is identified as enabling more convincing impersonations, scaled production of fake reviews, more evasive deceptive content, and faster adaptation to detection systems.[410]

Platform by Platform Overview

In addition to the general trends identified above, the table below summarises the analysis of each of the publicly available SRAs by VLOPs and VLOSEs in relation to financial scam behaviour. For reference, only the most recent versions of the reports (i.e., from 2025) have been included in the table below. An ‘X’ appears where the service provider explicitly recognises the risk category as a (systemic or inherent) risk in its assessment. If the risk behaviour is only mentioned tangentially, or as part of the mitigation/enforcement tooling, or the background context, it is marked with ‘*’. Where the platform did not identify this risk in its report, the cells are left blank.

[404] AliExpress, Facebook, Instagram, Snapchat 2025 Systemic Risk Assessment Reports.

[405] AliExpress, Amazon, Zalando, Shein, Google, TikTok 2025 Systemic Risk Assessment Reports.

[406] Amazon Store 2025 Systemic Risk Assessment Report.

[407] AliExpress 2025 Systemic Risk Assessment Report.

[408] Zalando 2025 Systemic Risk Assessment Report.

[409] AliExpress, Apple AppStore, Bing, Booking.com, Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[410] ibid.

It should be noted, as a methodological caveat, that blank cells are not to be construed as indicative of deficiencies in the risk assessments conducted by designated service providers. Rather, the absence of reported systemic risk in respect of certain services may reflect the fact that their general profile or core functionalities are of limited relevance to the phenomenon of online financial scams. Therefore, the table below should only be understood as a neutral overview of the findings publicly reported by designated service providers.

For each risk category, the table maps both the inherent and residual level of risk, as reported by the designated service providers. For accuracy, the table uses the terminology used by each provider in their report, which may lead to divergences in the evaluation of the level of risk. In some instances, a clear evaluation of the level of risk (inherent or residual) could not be identified – this is marked as ‘n/a’.

Table 3 - Overview of systemic risks related to financial scams as identified by designated service providers[411]

Platform	Inauthentic identity & account manipulation	Inherent	Residual	Deceptive commercial content	Inherent	Residual	Fraud via private messaging	Inherent	Residual	Illegal or counterfeit goods	Inherent	Residual	AI as a scam amplifier	Inherent	Residual
AliExpress	X	High	Medium	X (listing, reviews, ads)	High	Medium	X (chat misuse)	High	Medium	X	High	Medium	X	High	Medium
Amazon Store	*	n/a	n/a	X (product listings)	n/a	n/a				X	n/a	n/a			
Apple App Store	*	n/a	n/a	X (ads, reviews, app pages)	High	Low							X	High	Low
Bing	X	High	Low	X (ads, deceptive practices)	High	Low							X	High	Moderate
Booking.com	X	Moderate	n/a	X (fraudulent listings)	Moderate	n/a							X	Moderate	Stable
Facebook	X	Very High	Medium	X (deceptive ads/content)	Very High	High	X (redirection)	Very high	Moderate				X	Very high	High
Google Search	X	n/a	Low	X (unfair commercial practices)	n/a	Elevated				X	n/a	Elevated			
Google Play	*	n/a	Lower	X (manipulated ratings/reviews)	n/a	Low									
Google Maps	*	n/a	n/a	X (fake reviews and business info)	n/a	Low									
Google Shopping	*	n/a	Lower	X (inaccurate product representations)	n/a	Low				X	n/a	Low			
YouTube	*	n/a	n/a	X (scam content, ads)	n/a	n/a							X	n/a	n/a

[411] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

Platform	Inauthentic identity & account manipulation	Inherent	Residual	Deceptive commercial content	Inherent	Residual	Fraud via private messaging	Inherent	Residual	Illegal or counterfeit goods	Inherent	Residual	AI as a scam amplifier	Inherent	Residual
Instagram	X	Very high	Medium	X (deceptive content)	Very high	High	X (DM-based fraud)	Very high	High				X	High	Medium
LinkedIn	X	High	Moderate	X (fraudulent ads/posts)	High	Moderate	X (private messages)	High	Moderate						
Pinterest	X	Medium	Low	X	Medium	Low				X	Medium	Low			
Shein	*	n/a	Low	X (listings, reviews)	n/a	Low medium				X	n/a	Low medium			
Snapchat[412]	X	Level 2		X (ads)	Level 3		X	Level 3							
Temu	X	Low	Low	X (listings, reviews)	Medium-high	Medium	X (chat misuse)	Medium-high	Medium						
TikTok	X	Medium	Medium	X (scam content)	Medium-high	Medium				X	Medium	Medium			
X	X	High	Low	X (ads, scams)	High	Low	X (DMs misuse)			X	High	Low			
XNXX	*	n/a	n/a	X (deceptive advertising hidden charges)	Medium	Low				X (counterfeit material)	High	Medium	X	n/a	n/a
XVideos	X	Medium	Low	X (ads)	Medium	Low									
Zalando	*	n/a	n/a	X (product information)	Very low	n/a				X	Very low	n/a			
Pornhub															
Wikipedia															

[412] Please note that Snapchat does not differentiate between inherent and residual risks in its methodology.

3.2. Cross-platform considerations

Risk factors on VLOPs and VLOSEs are aggravated through specific vectors defining the operations and behaviours adopted by scammers, including migratory patterns across different environments, adaptive evolutions of the scam cycles, reliance on operational tools and social engineering methods, as well as external criminal infrastructures. The following sections assess these factors, starting with cross-platform migration patterns.

3.2.1. Cross-platform pathways

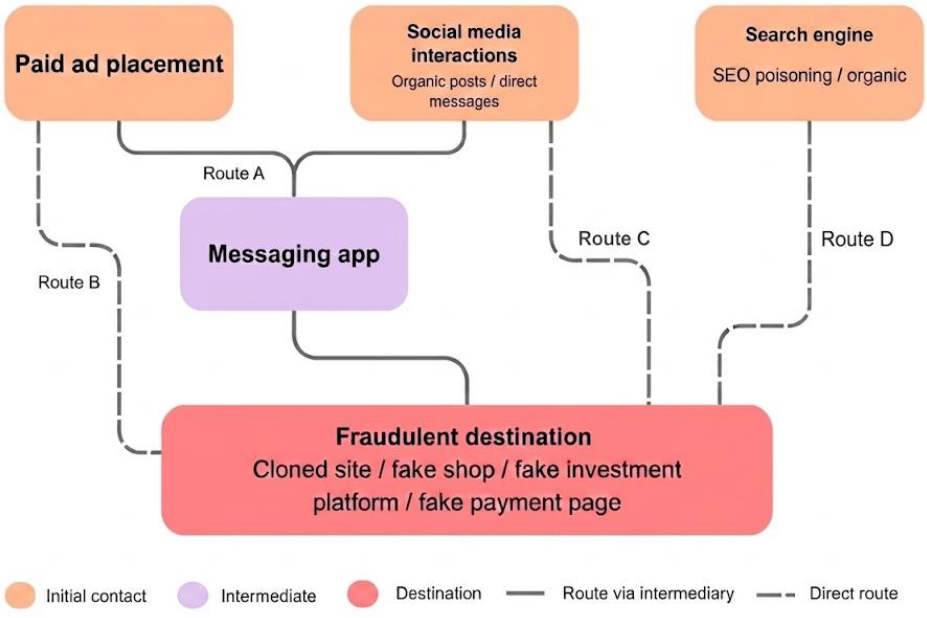
Online financial scams typically involve **a cross-platform chain of interactions**. Most commonly, these pathways originate in the use of paid ad placements, which generate an initial, high-visibility contact point that redirects the victim to other environments through which the scam is operated.

Two pathways are identified pursuant to interaction with a fraudulent ad. Under the first model, scammers use a paid ad to attract the victim's attention, then redirect them to a messaging application. From there, scammers lead victims to a fake website or payment service. The second model is similar, but shorter: the ad leads directly to a fraudulent website, omitting the private messaging step.

Another variant of this sequence replaces the paid ad placement with social media interactions (including direct messaging) as the first point of contact with a potential victim, leading to either a fake website or a fake payment service. Less frequently, victims may directly access these destinations through a first contact via search engine results.

The figure below indicates these pathways, which underscore most financial scam types discussed in this report.

Figure 2 - Cross-service pathways



Source: Authors' elaboration.

In migrating from the environment of social media platforms and paid ad placements, encrypted messaging applications function as a potential bridge between the initial contact and the eventual financial extraction.[413] Their use is reported by survey respondents from six Member States and is described as particularly prominent in the context of investment fraud.[414]

Victims may also reach fraudulent websites as an initial contact point when they surface directly in search engine results, through two complementary mechanisms: paid search placements and manipulated organic search results, as described above under Section 3.1.

Through these initial contact points (i.e., fraudulent ads, social media interactions or search engine results), victims are redirected to fraudulent websites, which constitute central operational tools across most types of online financial scams identified in this report, and which are further discussed under Section 3.2.5. below.

The cross-service pathways described above are generally applicable across all types of online financial scams described in this report. The following paragraphs briefly describe how each type of financial scam unfolds across this cross-platform landscape.

In operating traditional investment scams, fraudsters rely on multiple routes. Routes B and D in Figure 2 are prevalent, with paid ad placements on social media platforms and manipulated search engine results directing victims straight to fake trading platforms, cloned investment sites, or fake comparison websites.[415] Route A in Figure 2 also operates through social media interactions, where fraudsters use organic posts impersonating finfluencers or celebrities to initiate contact, before moving the conversation to messaging apps such as WhatsApp, where trust is built, and victims are ultimately redirected to fraudulent investment platforms.[416] A similar trend is observed in relation to cryptocurrency scams, with social media platforms such as Instagram, YouTube, TikTok and X used for paid advertising that directs victims directly to spoofed websites, fake wallets, or fake exchanges.[417] Route A is particularly evident in romance baiting, where initial contact through social media organic posts or direct messages

[413] Multi-stakeholder Workshop on Online Financial Scams.

[414] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[415] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”; Finans Danmark, Styrket bekæmpelse af digital svindel - Svindel Task Forcens 18 anbefalinger (2024), available at: https://www.ft.dk/samling/20241/almdel/ERU/bilag/81/2948819/index.htm.

[416] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”; Jingjia Xiao, Qing Xiao and Hong Shen, “It felt real” victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680; Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Investitionen in Kryptowerte und der Einfluss sozialer Medien auf das Anlageverhalten (2026), available at: https://www.bafin.de/DE/Aufsicht/Fokusrisiken/Fokusrisiken_2026/RIF_verbraucher_sozialemedien/RIF_verbraucher_sozialemedien_node.html;jsessionid=7482B626CD4BA5A50D21116827D3E0A2.internet012

[417] Gen, Gen Q4/2024 Threat Report (2024), available at: https://www.gendigital.com/blog/insights/reports/threat-report-q4-2024; Interpol, Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf; Competition and Consumer Protection Commission (CPCC), Scams – Real cases, real consequences: A collection of case studies and lessons for consumers (2025), available at: https://www.ccpc.ie/consumers/wp-content/uploads/sites/2/2025/11/Scams-Real-cases-real-consequences-CCPC.pdf; Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545

transitions to sustained communication via messaging applications, before victims are directed to fake trading or staking platforms.[418]

Romance scams primarily follow Route A; fraudsters establish initial contact through organic posts or direct messages on social media platforms and online dating services, before migrating communication to messaging apps where the trust-building and emotional manipulation techniques described in Section 3.2.5 take place over extended periods.[419] The fraudulent destination in this context is typically a fake payment page or fraudulent transfer mechanism, reached after the victim is persuaded to send funds under fabricated pretexts such as medical emergencies, trauma, or financial distress.[420]

For undelivered products and counterfeits scams, perpetrators mainly operate via Routes B and D. Paid ad placements direct victims straight to fake webshops, while manipulated search engine results bring victims directly to fraudulent storefronts.[421] In some cases, Route C is also relied on, particularly via live broadcasts or stories with hidden links redirecting victims to external fake shops.[422] Similarly, health and wellness scams predominantly follow Routes B, C and D, with limited evidence of Route A playing a role in this type of scam.[423]

---

[418] Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670.

[419] Matthew Edwards, Online sextortion: Characteristics of offences from a decade of community reporting (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000386; Heidi Wilcox and Maumita Bhattacharya, A human dimension of hacking: Social engineering through social media (2020), available at: https://arxiv.org/pdf/2005.04049; Janneke M Schokkenbroek and Thom Snaphaan, Love as Bait: A Scoping Review and Crime Script Analysis of Online Romance Scams (2025), available at: https://journals.sagepub.com/doi/10.1177/15248380251361046; Amy Lim and Kyung-shick Choi, Modus operandi and blockchain analysis of romance scams: Cryptocurrency-driven victimization (2025), available at: https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1220&context=ijcic ; Jingjia Xiao, Qing Xiao and Hong Shen, "It felt real" victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[420] Cassandra Cross and Karen Holt, To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581; Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en.

[421] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA"; Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar;

[422] Union des Fabricants (UNIFAB), Counterfeiting & Organised Crime (2025), available at: https://www.unifab.com/wp-content/uploads/2025/06/UNIFAB_Contrefacon-Criminalite_ENGLISH_VDEF_03062025.pdf; European Union Intellectual Property Office, Monitoring and analysing social media in relation to IP infringement (2021), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Monitoring_and_analysing_social_media_in_relation_to_IPR_Infringement_Report/2021_Monitoring_and_analysing_social_media_in_relation_to_IPR_Infringement_Report_FullR_en.pdf.

[423] Interview 6; corroborated by Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/The_threat_of_pharmaceutical_crime_in_the_EU_and_beyond.pdf; AI Forensics Meta Ads: A Pill Hard to Swallow (2024), available at: https://aiforensics.org/uploads/meta_health.pdf; Health Products Regulatory Authority (HPRA), Urgent warning of fraudulent websites and adverts promoting illegal medicines (2025), available at:

As part of event ticket scams, fraudsters make use of both Routes A and B. Route B operates through paid search engine advertising, where unauthorised resale platforms appear above organic results, and through social media paid ads.[424] Route A is also documented, with fraudsters using social media organic posts and comments on event-related pages to initiate contact, before moving negotiation to messaging apps or direct message functions, where fake or stolen tickets are exchanged and fraudulent payments completed.[425]

Insurance scams primarily follow Route A. Ghost brokers initiate contact through organic social media posts advertising discounted policies, before shifting communication to private messaging apps to conduct negotiations and deliver fraudulent insurance certificates.[426] Route B also applies where paid ad spoofing is used to boost cloned insurer websites to the top of search engine results, directing victims there directly.[427]

In relation to loan and credit offer scams, multiple Routes have been documented. Interviewees indicated that Route B operates through paid social media advertising, while manipulated search engine results surface fake comparison websites listing fraudulent loan offers (Route D).[428] Route A involves direct messages or unsolicited contact on social media platforms, which then migrate to messaging environments where victims are manipulated into submitting applications and ultimately directed to fraudulent payment pages to pay the upfront fee.[429]

Charity scams and fraudulent crowdfunding operate predominantly via Routes B and D, with fraudulent charity campaigns disseminated through paid social media posts or surfaced through manipulated search engine results, directing victims straight to fake donation websites that mimic the visual identity of reputable charities.[430] Organic social media sharing of

https://www.hpra.ie/news-events/news/article/urgent-warning-of-fraudulent-websites-and-adverts-promoting-illegal-medicines.

[424] FEAT, 1750 Potentially Fraudulent Tickets Offered for Radiohead's European Tour (2025), available at: https://www.feat-alliance.org/2025/09/17/1750-potentially-fraudulent-tickets-offered-for-radioheads-european-tour/; Proofpoint, Security Brief: Scammers Create Fraudulent Olympics Ticketing Websites (2024), available at: https://www.proofpoint.com/us/blog/threat-insight/security-brief-scammers-create-fraudulent-olympics-ticketing-websites?&web_view=true; Nederlandse Politie, Politie waarschuwt met nepwebsite voor ticketfraude (2026), available at: https://www.politie.nl/nieuws/2026/januari/15/politie-waarschuwt-met-nepwebsite-voor-ticketfraude.html.

[425] Take Five, Ticket scams, available at: https://www.takefive-stopfraud.org.uk/protect-yourself/ticket-scams/.

[426] Insurance Europe, Insurance Europe response to EC consultation on online fraud (2026), available at: https://www.insuranceeurope.eu/mediaitem/c356079f-c353-4754-a049-1a0054e0b29b/Insurance+Europe+response+to+EC+consultation+on+online+fraud.pdf?inline=1; The Guardian, 'Ghost broking': cut-price car insurance isn't all it seems (2025), available at: https://www.theguardian.com/money/2025/nov/16/ghost-broking-cut-price-car-insurance-scam-watch.

[427] The ABI, Online Fraud, available at: https://www.abi.org.uk/products-and-issues/topics-and-issues/fraud/online-fraud/.

[428] Interviews 2, 4.

[429] Financial Services and Market Authority, Received an interesting credit offer? Be careful! (2025), available at: https://www.fsma.be/en/warnings/received-interesting-credit-offer-be-careful.https://www.fsma.be/en/warnings/received-interesting-credit-offer-be-careful.

[430] Europol, Online fraud schemes – A web of deceit (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/e914d7fe-b429-11ee-b164-01aa75ed71a1/language-en

fraudulent crowdfunding campaigns (Route C) also serves as a direct pathway to fraudulent collection pages on platforms such as GoFundMe.

Lastly, in relation to unexpected gain scams, Route B dominates, with pop-up advertisements, paid placements, and app store listings directing victims directly to fake casino platforms, fraudulent betting sites, or fake prize-claiming pages.[431] An interviewee indicated that social media advertising using deepfakes or impersonations of legitimate platforms drives direct traffic to fraudulent destinations, with no messaging app intermediary typically involved.[432]

Whereas the pathways described above are generally applicable across the identified scam types, **there are also exceptions**, as described below.

Rental scams may make use of the pathways described above, or not, depending on the type of accommodation sought after. For longer-term rentals, Route A is common: fraudsters post on social media platforms, initiate contact, and then move communication to direct messaging to persuade victims to pay deposits for non-existent properties, with fraudulent payment pages serving as the final destination.[433] However, for vacation rentals, the scam is typically confined within the environment of the accommodation platform, with potential migration to private communication channels.[434]

Subscription scams represent a partial exception to the common pathway in that the fraudulent destination is often a legitimate-appearing service rather than an overtly fake platform, and the harm arises not from a single fraudulent transaction but from the ongoing extraction of recurring payments.[435] While paid search advertising is used to drive victims directly to fraudulent subscription pages (consistent with Route B), the deceptive mechanism lies in hidden contractual terms, dark patterns, and deliberately complex cancellation processes embedded within the destination itself.[436]

Artificial streaming scams deviate significantly from the common pathways in that there is no fraudulent destination to which individuals are directed. Instead, fraudsters operate entirely within legitimate streaming and social media platforms, deploying automated bots and scripts to artificially inflate engagement metrics.[437]

---

[431] Debunk, Debunk.org Trusted Flagger 2025 Report (2026), available at: https://www.debunk.org/debunk-org-trusted-flagger-2025-report.

[432] Interview 6.

[433] Sophie Van Der Zee et al., The gift of the gab: Are rental scammers skilled at the art of persuasion? (2019), available at: https://arxiv.org/abs/1911.08253.

[434] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”; Julie Reid, Delusive speech in the sharing economy: Scam Inc. (2025), available at: https://www.taylorfrancis.com/books/mono/10.4324/9781003513995/delusive-speech-sharing-economy-julie-reid.

[435] Sheil et al., Staying at the Roach Motel: Cross-Country Analysis of Manipulative Subscription and Cancellation Flows (2024), available at: https://arxiv.org/pdf/2309.17145.

[436] ÖIAT, Verbreitung von Abo-Fallen durch Google Ads (2026), available at: https://www.watchlist-internet.at/fileadmin/files/Abo-Fallen/Google-Policy-Paper.pdf.

[437] Interview 8; see also Andrew Chu et al., Behind the Tube: Exploitative Monetization of Content on YouTube (2022), available at: https://www.usenix.org/system/files/sec22-chu.pdf/

Employment scams are also unique in terms of their cross-platform migration patterns. Fake job scams mainly occur on recruitment platforms, with documented reports of users receiving fake job offers.[438] Scammers post fake job openings to which victims respond, or they directly contact victims, sending them private messages with job offers. The specific infrastructure of online recruitment sites gives fraudsters an advantage, as their fraudulent job postings blend in with the legitimate ones, rendering it hard to detect job scams.[439] Platforms through which jobseekers can also present their profiles and professional achievements also enable scammers to more easily identify potential targets – for example, it is posited that the #open to work' profile graphic can increase the likelihood of being approached by scammers.[440]

Money mule recruitment occupies an ambiguous position. While initial contact does follow recognisable patterns (job advertisements on recruitment platforms or social media posts, consistent with Route C, or direct outreach through fake profiles, consistent with Route A), the fraudulent destination is not a cloned site or fake payment page but rather the victim's own bank account, which is used as a conduit for laundering illicit funds.[441] Communication typically migrates from public platforms to encrypted messaging apps, following Route A, but the objective is not to extract a payment from the victim, but to recruit them as an unwitting participant in a broader criminal operation.

While DM to Collab scams do involve an initial contact and a financial request, they deviate from the common pathway in that the entire scam is typically contained within the social media platform itself, with social media interactions used as a first point of contact, and direct messaging functioning simultaneously as the intermediary space for trust-building and the point of payment solicitation. Unlike the standard Route A model, victims are rarely redirected to an external fraudulent destination; instead, the payment is solicited directly within the social media platform messaging environment.[442]

The cross-platform routes described above are designed to evade detection and amplify the reach of fraudulent behaviours; this objective is also achieved through perpetual adaptation and hybridisation in the design of financial scams, as described in the following section.

---

[438] Vice, Scammers Are Sending Fake Job Offers on LinkedIn (2021), available at: https://www.vice.com/en/article/scammers-are-sending-fake-job-offers-on-linkedin/.

[439] Syed Mahbub and Eric Pardede, Using Contextual Features for Online Recruitment Fraud Detection (2018), available at: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1247&context=isd2014.

[440] Forbes, Job Seekers: Be Careful Using LinkedIn's New "Open To Work" Feature (2020), available at: https://www.forbes.com/sites/roberthellmann/2020/07/20/job-seekers-be-careful-using-linkedins-new-open-to-work-feature/.

[441] Europol, Money Muling (2025), available at: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling; Ehi Eric Esoimeme, Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules (2021), available at: https://www.emerald.com/jmlc/article-abstract/24/1/201/241861/Identifying-and-reducing-the-money-laundering?redirectedFrom=fulltext; UK Finance, Money mule recruiters use fake online job adverts to target "Generation Covid", available at: https://www.ukfinance.org.uk/press/press-release/money-mule-recruiters-use-fake-online-job-adverts-to-target-generation-covid.

[442] Raj Vardhan et al., #DM-Me: Susceptibility to Direct Messaging-Based Scams (2023), available at: https://dl.acm.org/doi/pdf/10.1145/3579856.3582815; VICE, Those 'DM to Collab' Instagram Messages Are Probably a Scam (2021), available at: https://www.vice.com/en/article/dm-to-collab-instagram-messages-scam/.

3.2.2. Adaptable nature of scammers

There is broad agreement amongst the stakeholders interviewed that **scammers adapt rapidly to emerging trends by aligning their tactics with the different topics, formats, or platforms that are currently trending**.[443] One interviewee indicated that this adaptability operates across multiple dimensions, including both the strategic selection of platforms based on the target audience sought, as well as the deliberate use of trending content or of current socio-political events to maximise visibility and reach.[444] By way of example, event ticket scams often focus their attention on high-demand and trending events, such as the Olympics, Champions League finals, Taylor Swift or Oasis tours.[445] Moreover, another stakeholder underlined that this trend-driven dissemination is facilitated by automated tools, including bots and AI-based tools. [446]

This adaptive logic is not limited to content, but it also extends to targeting and to the structure of scams. The personalisation of fraudulent content through profiling techniques was identified as a key driver of scam content. One interviewee noted that **observing what content users post about or interact with enables scammers to tailor messages to specific user characteristics and current interests, thereby increasing credibility and engagement**.[447] Another interviewee highlighted that the choice of platform is in itself a targeting strategy, claiming that 'if the fraudster wishes to go after younger victims, then TikTok would be the platform of choice, while if the target to be reached is users over 50 years old, then Facebook would be the preferred option'.[448]

Another stakeholder stated that an increasingly important dimension of the operational and behavioural landscape of financial scams is the **adjustment of the very structure of scam models in response to increased user awareness and platform dynamics**.[449] Romance baiting (see Section 2.2.2) exemplifies this trend through deliberate hybridisation. These broader trends of hybridisation are an adaptive response by fraudsters. By combining elements from different scam categories, they construct schemes that do not neatly fit the warning patterns described by counter-scam awareness campaigns, maintaining a strategic advantage over both victim recognition and enforcement categorisation.

These hybridisation patterns rely on the combination of multiple operational tools, which may traditionally be associated with different types of online financial scams. The following section enlists some of the most common tools, the types of scams they are associated with and the platforms on which they are deployed.

[443] Interviews 3, 4, 7.

[444] Interview 1.

[445] Nederlandse Politie, Politie waarschuwt met nepwebsite voor ticketfraude (2026), available at: https://www.politie.nl/nieuws/2026/januari/15/politie-waarschuwt-met-nepwebsite-voor-ticketfraude.html.

[446] Interview 8.

[447] Interview 7.

[448] Interview 1.

[449] Interview 4.

3.2.3. Operational tools

Scammers rely on a wide range of operational tools in the execution of online financial scams, including technically sophisticated instruments such as deepfakes, malware, fake websites and AI-generated content. This section consolidates the operational tools identified across all scam typologies covered in this report, linking them to specific types of scams and platform features. Where the use of these tools is facilitated through risk factors stemming from platform functions or design, this is indicated with reference to Section 3.1, which discusses this aspect in more detail. Otherwise, if no information or correlation exists between an operational tool and a platform function, this aspect is omitted from the paragraph.

Impersonation is the foundational operational technique across virtually all categories of financial scams identified as part of this report. It takes multiple forms: the impersonation of public figures, celebrities, and financial authorities to establish credibility for investment offers, the cloning of legitimate financial institutions, lenders, insurance brokers, and public organisations to induce trust, the creation of fake recruiter or employer profiles to deceive jobseekers, and the fabrication of romantic or social personas to establish emotional relationships with victims.[450] Beyond impersonating figures, scammers also rely on institutional impersonation, adopting the names, logos, branding and communication styles of EU institutions, national authorities, legitimate companies or public organisations.[451] For example, Debunk.org submitted 105 reports to Facebook and Instagram concerning a scheme impersonating Interpol, Europol, and EU institutions, which resulted in the removal of 874 pages and 29,156 ads, which had, however, already reached an estimated audience of 30 million users across the EU before removal.[452] However, information on the actual success rate of these fraudulent ads is not available. As discussed above under Section 3.1, the frequent use of impersonating accounts is encountered across a range of platforms (social media, marketplaces) and may be facilitated by shortcomings in the identity verification processes of online platforms. Impersonation in ad placements is common both in terms of the account placing the ad and in its content; this is encountered both on social media and online search engines, which are the primary environments for ad placement.

The creation of **fraudulent or cloned websites** is among the most widely deployed operational tools across scam typologies. Fraudulent websites take several distinct forms depending on the type of scams they support. The following paragraph enlists the most common types of fraudulent websites used in the operationalisation of financial scams, followed by a discussion on the infrastructure behind the creation of these websites. Although they may vary in type, fake websites primarily reach their victims through ad placements or

[450] Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/; Financial Services and Market Authority, Received an interesting credit offer? Be careful! (2025), available at: https://www.fsma.be/en/warnings/received-interesting-credit-offer-be-careful; Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en; Rajvardhan Oak and Zubair Shafiq, “Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf.

[451] Financial Services and Market Authority, Cloned firms: theft of the identity of authorized companies, available at: https://www.fsma.be/en/cloned-firms-theft-identity-authorized-companies.

[452] Debunk, Debunk.org Trusted Flagger 2025 Report (2026), available at: https://www.debunk.org/debunk-org-trusted-flagger-2025-report.

search engine results.[453] This may be facilitated by shortcomings in the advertising systems of online platforms and search engines, and by search engine ranking algorithms that do not prioritise high-quality results.

Cloned websites are near-identical replicas of legitimate platforms, with subtle modifications to URL, branding or language that are difficult for victims to detect.[454] They are used across a wide range of scam types. Cloned banking and investment platform sites are used to harvest credentials and redirect payments in investment fraud, while cloned insurance broker websites are used to sell fake policies as part of insurance fraud. Moreover, cloned e-commerce sites are used to collect payments for products that will never be delivered, whereas cloned news websites are used to lend editorial legitimacy to fraudulent investment offers. A particularly sophisticated example of the use of cloned websites is described above, under Section 2.3, in relation to rental scams.

Fake webshops and ghost stores are fraudulent e-commerce websites that simulate legitimate online retail operations, offering products at unusually low prices, collecting payments, and then failing to deliver. As these types of websites are primarily used as part of undelivered product or counterfeit scams, a commercial website-building platform is commonly used to provide professional storefront appearances.[455]

Fake trading and investment platforms simulate the interface of legitimate financial trading services, including fabricated dashboards, account statements, and real-time price feeds, to convince victims that their funds are being actively managed. These infrastructures combine entirely fabricated trading interfaces with the appropriation of legitimate platform features, designs, and logos.[456] Survey respondents indicate that AI is increasingly used to generate entirely fictitious transaction histories at realistic prices, making the deception harder to detect.[457] This type of fake website is common in investment scams and in romance baiting as a form of social proof, reinforcing the legitimacy of the transactions in the eyes of the victim. Victims are directed to platforms that simulate the interface of legitimate trading environments, displaying fabricated returns, real-time price movements, and detailed portfolio statements to sustain the illusion of genuine activity.[458] When victims attempt to withdraw funds, the platform imposes further fees or taxes, or simply becomes inaccessible.

Fake comparison, aggregator, or news websites present themselves as impartial evaluators of financial products, steering visitors towards fraudulent options.[459] Fraudsters also use fake

[453] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[454] ibid.

[455] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”; Platon Kotzias et al., Scamdog Millionaire : Detecting E-commerce Scams in the Wild (2023), available at: https://dl.acm.org/doi/pdf/10.1145/3627106.3627184.

[456] Interview 4; see also Jingjia Xiao, Qing Xiao and Hong Shen, “It felt real” victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[457] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[458] Rajvardhan Oak and Zubair Shafiq, “Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf.

[459] Interview 4.

websites that appear to offer news, analysis, or endorsements in order to build credibility for the scam being promoted - the framing of the content as journalism rather than advertising is meant to induce a higher sense of legitimacy. These sites are designed to mimic the editorial appearance of established media outlets, complete with fabricated journalist bylines and fictitious reader comments.[460] This type of website is used as part of investment scams, insurance fraud, loan/credit offer scams, or health and wellness scams.

The creation of fraudulent websites relies on a layer of supporting infrastructure that is itself deliberately selected and exploited by criminal actors. This **website-creation infrastructure** encompasses web hosting services, domain name registrars, commercial website-building platforms, content delivery networks used for anonymisation, and SEO manipulation tools. Collectively, these components enable fraudsters to construct credible online presences at speed and scale, while remaining difficult to identify and take down. Fraudulent websites are hosted on commercial web hosting providers, with deceptive or misleading domain names designed to generate confusion with legitimate brands or institutions.[461] Website-creation infrastructure may be aimed at manipulating search engine results, as described below in relation to domain registration.

The tactic of acquiring previously expired domain names is a further infrastructure-level technique. Fraudsters rely on domain names that previously belonged to legitimate websites and have since lapsed, deliberately targeting those with an established track record of positive signals in search engine rankings.[462] By inheriting the domain's organic search ranking, fraudsters ensure that their fraudulent site is surfaced to users as a trusted, high-ranking result.[463] SEO poisoning complements this approach: malicious code is installed into compromised websites to intercept server requests and return fabricated content, causing search engines to index fraudulently generated pages as if they were part of established legitimate sites.[464]

The ‘infrastructure-as-a-service’ model represents the most industrialised form of fraudulent website creation. Under this model, a core technical team manages the hosting infrastructure, domain registration, and payment processing architecture, while a decentralised network of operators runs individual fraudulent shops or investment platforms built on top of it (see case study C in Section 6.3 for a detailed analysis of this model).[465]

Phishing, vishing and smishing techniques appear as recurring operational tools across the online financial scams identified above, serving the shared purpose of imitating legitimate communications or entities to obtain sensitive information or redirect victims to fraudulent

[460] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[461] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[462] Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar.

[463] Makoto Shimamura, Uncovering Black-hat SEO based fake E-commerce scam groups from their redirectors and websites (2025), available at: https://arxiv.org/html/2505.21021v1.

[464] ibid.

[465] Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar.

platforms.[466] These techniques involve impersonating trusted entities through email, telephone calls, or private messages to extract credentials, personal data, or payments from victims. As such, this tool is mainly deployed through private communication channels on social media or online marketplaces that implement this feature. Their prominence is explained by their reach and speed; for example, an interviewee indicated that phishing campaigns can be developed and deployed rapidly, reaching broad portions of the population before detection and takedown can occur.[467] Phishing was further highlighted as a tool that enables offenders to perpetrate various forms of online scams without requiring specific expertise.[468] Phishing kits, including ready-made websites designed to mimic legitimate organisations and services, are increasingly being sold as a service.[469]

Spear phishing is a targeted variant of phishing in which the attacker accesses data leaks to identify potential victims, using contextual details to personalise their approach and craft highly credible messages.[470] The use of these techniques is popularised through **'phishing-as-a-service'** toolkits provided by organised crime vendors.[471]

In the context of romance scams, perpetrators rely on targeted spear phishing, whereby victims are identified and approached through social media by using personalised messages, then tricked into surrendering personal data such as passwords or financial credentials, with the deceptive framing of a trusted intimate relationship providing the social cover for such requests.[472] In rental scams, fraudsters deploy phishing in combination with impersonation of real hosts or landlords, as illustrated in the attack on Booking.com previously described in Section 2.3. Across DM to Collab scams targeting content creators, phishing techniques add a layer of sophistication to brand impersonation schemes.

Advance fee mechanisms constitute a recurring operational tool across multiple scam typologies, exploiting the victim's anticipation of a larger benefit to justify an upfront payment that is never recovered. In investment scams (both traditional and crypto-based), advance-fee mechanisms are commonly deployed, requiring victims to transfer money in anticipation of receiving a larger financial benefit.[473] Romance scams and romance baiting frequently employ advance-fee mechanisms, particularly in the context of fabricated emergencies such as medical crises, trauma, or financial distress, which are used to justify urgent financial requests

[466] Interview 2.

[467] Interview 4.

[468] Europol, Decoding the EU's Most Threatening Criminal Networks – Issue 2: The Blueprint of Criminal Opportunism (2026) available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Blueprint-of-criminal-opportunism.pdf.

[469] Ibid.

[470] Interview 7; see also ENISA, Threat Landscape 2024 (2024), available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[471] Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/.

[472] Matthew Anderson et al., Exploring the roles played by trust and technology in the online investment fraud victimisation process (2024) available at: https://journals.sagepub.com/doi/pdf/10.1177/26338076241248176.

[473] Antonis Papasavva et al., Applications of AI-Based Models for Online Fraud Detection and Analysis (2025) available at: https://link.springer.com/content/pdf/10.1186/s40163-025-00248-8.pdf; Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545;

framed within the perceived intimacy of the relationship.[474] In loan and credit offer scams, the advance-fee structure is central to the scheme: once the victim submits an application and receives fictitious approval, fraudsters request an upfront fee, after which they disappear, leaving the victim without the promised funds and without any means of recovering the payment.[475] In rental scams, longer-term variants operate as a form of advance fee fraud, with fraudsters impersonating landlords and persuading victims to pay a deposit for a property they have never visited and which most likely does not exist.[476]

Technical malware tools play a more targeted role in the financial scam ecosystem. Ransomware infects victims' devices, encrypts their data, and demands payment before access is restored.[477] Cryptologgers are a category of malware designed specifically to steal credentials associated with cryptocurrency accounts or to intercept private keys required to transfer crypto-assets, typically operating as a transparent interface layer while the user navigates relevant websites.[478] More broadly, malware and spyware tools, botnets, man-in-the-middle attacks, and techniques exploiting system vulnerabilities have been identified as part of the technical toolkit used by financially motivated cyber criminals.[479] These tools are usually deployed outside the environment of designated services, either through private communication channels or through fraudulent websites.

KYC manipulation or circumvention is another operational tool frequently used by fraudsters in the context of investment scams.[480] Scammers exploit weaknesses such as fragmented vendor stacks –the use of multiple vendors by online platforms for different

[474] Alexander Bilz et al., Tainted Love: a Systematic Literature Review of Online Romance Scam Research (2023), available at: https://academic.oup.com/iwc/article/35/6/773/7331428; Janneke M Schokkenbroek and Thom Snaphaan, Love as Bait: A Scoping Review and Crime Script Analysis of Online Romance Scams (2025), available at: https://journals.sagepub.com/doi/10.1177/15248380251361046; Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670.

[475] Financial Services and Market Authority, Received an interesting credit offer? Be careful! (2025), available at: https://www.fsma.be/en/warnings/received-interesting-credit-offer-be-careful; L'Autorité de contrôle prudentiel et de résolution (ACPR), L'ACPR met en garde le public contre la multiplication de fausses offres de prêt immobilier ou de rachat de crédit proposées par des individus usurpant l'identité de courtiers et d'établissements de crédit (2024), available at: https://acpr.banque-france.fr/fr/communiques-de-presse/lacpr-met-en-garde-le-public-contre-la-multiplication-de-fausses-offres-de-pret-immobilier-ou-de

[476] Sophie Van Der Zee et al., The gift of the gab: Are rental scammers skilled at the art of persuasion? (2019), available at: https://arxiv.org/abs/1911.08253.

[477] Interview 1; see also Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545.

[478] Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545.

[479] Interview 1; corroborated by Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en; Europol, 2023 IOCTA (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/238c0013-26a9-11ee-a2d3-01aa75ed71a1/language-en

[480] Samuel Aidoo, Customer Due Diligence (CDD) and Know Your Customer (KYC) (2025), available at: https://www.researchgate.net/profile/Samuel-Aidoo-2/publication/393884914_Customer_Due_Diligence_CDD_and_Know_Your_Customer_KYC/links/687eaca3ba8eac4f1727fcf8/Customer-Due-Diligence-CDD-and-Know-Your-Customer-KYC.pdf.

aspects of KYC (e.g., one for ID verification, another for liveness, a third for Anti-Money Laundering) creates data silos and integration complexities, allowing scammers to slip through the cracks.[481] Scammers also manage to circumvent the live checks through the use of deepfakes and AI-generated biometrics.[482] However, a key structural vulnerability also arises from the fact that many Know Your Customer (KYC) and trader verification systems rely at least in part on initial self-declaration by users; as a result, scammers may simply falsely declare themselves as non-traders or low-risk users to circumvent controls, making misrepresentation at the declaration stage itself a systemic issue. Compromised or fraudulently created identities may subsequently be used across institutional onboarding and compliance systems, including for the resale of verified accounts or to facilitate further criminal activities involving downstream victims.[483] KYC manipulation is mainly used in the context of online marketplaces or financial environments (e.g., trading platforms or banking environments).

Bot accounts and networks of fake profiles are also used as tools for different purposes. Inter alia, fraudsters use them to amplify the apparent credibility of fraudulent investment groups by populating them with simulated participants within the context of investment scams, to enable mass distribution of phishing messages and fraudulent collaboration offers (DM to Collab scams), or to replicate user engagement and behaviour online at a scale that would be impossible manually (artificial streaming scams).[484] Bots can generate contextually appropriate comments, participate in conversations, and even vary their behaviours to evade automated detection and human moderators.[485] An interviewee indicated that the software infrastructure required to automate these behaviours is frequently sold as a commercial product on black markets, availability which increases the scale of scam operations and lowers barriers to entry for actors without technical expertise.[486] Moreover, the price of acquiring and deploying bot accounts is marginal, as monitored by the Cambridge Online Trust and Safety Index platform, which tracks daily prices and the availability of fake SMS verified accounts across different types of online platforms.[487] The offering of such services and the increased presence of inauthentic accounts on online platforms point towards significant shortcomings in the identity verification process associated with account creation.

An emerging technical development observed by the stakeholders consulted is the use of '**link cloaking' techniques** that serve different content to different users who access a hyperlink

[481] ibid.

[482] Didit, Fraud Syndicates: How Organized Criminals Bypass KYC (2026), available at: https://didit.me/blog/fraud-syndicates-bypass-kyc/.

[483] Dock Labs, KYC fraud: 7 strategies to prevent KYC fraud (2026), available at: https://www.dock.io/post/kyc-fraud#what-is-kyc-fraud.

[484] Interview 8; see also Autorité des Marchés Financiers, Social Media Intelligence: Arnaques à l'investissement sur le web (2024), available at: https://www.amf-france.org/sites/institutionnel/files/private/2024-12/opinionway-pour-amf-les-arnaques-sur-le-web_octobre-2024_0.pdf; Dennis Assenmacher et al., Demystifying Social Bots: On the Intelligence of Automated Social Media Actors (2020), available at: https://journals.sagepub.com/doi/pdf/10.1177/2056305120939264; StreamCharts, The Hidden Cost of Viewbotting (2025), available at: https://streamscharts.com/reports/viewbotting-whitepaper.

[485] ibid.

[486] Interview 8.

[487] University of Cambridge, Cambridge Online Trust and Safety Index, available at: https://cotsi.org/platforms?view=map&platform=ig.

based on their identity or device characteristics.[488] When accessed by content moderation systems, automated crawlers, or bots, a cloaked link displays a harmless page; when accessed by a standard user, the same link redirects to a fraudulent website. An additional technological enabler is Voice over Internet Protocol (VoIP), which enables criminals to place high volumes of calls at low cost while concealing their location and facilitating caller ID spoofing. One stakeholder noted the emergence of a 'spoofing-as-a-service' business model enabling large-scale impersonation of trusted institutions.[489] Some Member States, including Italy and Finland, have started to employ countermeasures, including protocols for digital authentication of VoIP calls, query systems for real-time validation of caller location, blacklist management, and automated blocking capabilities.[490]

The impact and reach of these operational tools are enhanced through AI, as described below.

3.2.4. AI as an amplifying element

The growing role of automation is omnipresent across all types of online financial scams. What distinguishes the current scam landscape is not the novelty of scam types and of individual operational tools but the degree to which their **accessibility, scalability, and combination have been transformed by the availability of generative AI and automation infrastructure**.[491] In particular, AI enables more convincing impersonations, large-scale production of fabricated content, and faster iteration in response to moderation systems.[492] In this context, stakeholders have highlighted that generative AI has become a major component of scams and should be treated as a cross-category enforcement concern, with emerging threats including AI companions, SEO poisoning of large language models, and prompt injection that directs users to fraudulent websites.[493]

A central way AI amplifies scam risks is by **fabricating large-scale credibility signals**, most notably through deepfake technologies (meaning the use of AI to generate or manipulate video, audio, and images to fabricate or alter the appearance of real individuals).[494] One interviewee noted that the increasing sophistication of these tools makes early detection difficult even for trained observers.[495] In practice, deepfakes are used to produce fabricated endorsements by public figures, including celebrities, politicians, or business leaders, which

[488] Interview 5; Multi-stakeholder Workshop on Online Financial Scams.

[489] Interview 2.

[490] EUCPN, Postal and Cybersecurity Police Service ITA (2025), available at: https://eucpn.org/document/italy-the-criminal-implications-of-cli-spoofing; EUCPN, Scam call and payment fraud prevention FI (2025), available at: https://eucpn.org/sites/default/files/document/files/ECPA%20FI%20-%20Scam%20call%20and%20payment%20fraud%20prevention.pdf.

[491] Interview 8.

[492] Interview 2.

[493] Interviews 2, 8, 14; Multi-stakeholder Workshop on Online Financial Scams.

[494] Interviews 1, 2, 4, 5, 6; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA"; see also Europol, Decoding the EU's Most Threatening Criminal Networks – Issue 2: The Blueprint of Criminal Opportunism (2026) available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Blueprint-of-criminal-opportunism.pdf.

[495] Interview 5.

are then deployed in paid advertising to promote fraudulent investment platforms, gambling services, or cryptocurrency schemes.[496] Similar techniques are observed in other scam contexts: in health and wellness scams, for example, scammers rely on deepfake videos or otherwise AI-generated content impersonating doctors, public authorities, or media outlets to promote unapproved pharmaceutical products, leveraging perceived authority to gain consumer trust.[497]

Beyond visual manipulation, deepfakes extend to other areas. Voice cloning and AI-generated conversational agents are increasingly used in telephony and video-based scams to impersonate family members, managers, and financial advisors.[498] Generative AI can produce scripts, automate responses, and sustain multiple exchanges, enabling fraudsters to simulate human interactions and maintain contact with large numbers of victims.[499] Across scam types, these tools contribute to the objective of lowering the cost of personalised engagement while increasing perceived authenticity.

Another key dimension of AI as an amplifier is its role in **scaling scam content and infrastructure.** In the context of non-delivery scams, for instance, generative AI enables the rapid creation of convincing website content, product descriptions, and brand-consistent visual identities, substantially reducing the time and cost required to build fraudulent online shops. Fake storefronts can then be replicated and adapted at scale, making them more resilient to moderation and takedown measures. A similar logic applies to job-related scams, where AI is used to produce realistic job offers, company websites, LinkedIn profiles, and even to conduct interviews through deepfakes.[500] In both cases, AI facilitates the mass production of credible environments, making scalability easier and detection more difficult.

Additionally, AI enables the automation of engagement and platform manipulation, **allowing scammers to replicate not only static content but also dynamic signals of legitimacy**. By way of example, in streaming fraud, advances in AI development make it easier to automate both account creation and behavioural interactions, including comments, chat activity, and overall engagement.[501] One interviewee indicated that this practice has become

[496] Interview 6; see also Watchlist Internet, Die Evolution des Online-Betrugs: Vom klassischen Internetbetrug zur KI-gestützten Täuschung (2024), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Bericht_KI_und_Betrug_final.pdf; ÖIAT, Dubiose Werbung auf Meta-Plattformen: Wie Celebrity-Ärzte zur Bewerbung von Nahrungsergänzungsmitteln missbraucht werden (2025), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Safe-NEM-Bericht.pdf.

[497] Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/The_threat_of_pharmaceutical_crime_in_the_EU_and_beyond.pdf; Europol-EUIPO, Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact (2024), accessible at: https://www.europol.europa.eu/publications-events/publications/uncovering-ecosystem-of-intellectual-property-crime.

[498] Interview 7; Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[499] ibid.

[500] JobScamScore, Job Scam Statistics 2026 (2026), available at: https://jobscamscore.com/guides/job-scam-statistics; Internet Crime Complaint Center (IC3), Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions (2022), available at: https://www.ic3.gov/PSA/2022/psa220628.

[501] Dennis Assenmacher et al., Demystifying Social Bots: On the Intelligence of Automated Social Media Actors (2020), available at: https://journals.sagepub.com/doi/pdf/10.1177/2056305120939264.

increasingly prevalent, allowing fraudulent activity to be deeply embedded, reinforcing the appearance of authenticity.[502]

A further effect of generative AI relates to the **erosion of traditional detection signals**, as well as the expansion of personalised targeting. Before widespread AI availability, a common detection marker for users was the presence of linguistic or grammatical errors in fraudulent communications. One stakeholder claimed that generative AI effectively eliminates this signal, enabling grammatically correct and contextually appropriate communications in multiple languages.[503] However, this capability does not imply uniform levels of performance across languages; in fact, AI systems tend to perform better in high-resource languages, while outputs involving less-used languages may be less precise.[504] At the same time, AI enables the personalisation of fraudulent content based on profiling. By using AI to analyse potential victims' digital footprints, social media activity, and data leaks, fraudsters can develop targeted approaches that are more credible than generic mass-distribution attacks.[505]

Taken together, these developments indicate that **AI operates as an enabler across all platform types and scam categories,** making them more scalable and more convincing. As highlighted by stakeholders, this has accelerated the evolution of scammers' tactics, allowing them to swiftly develop new techniques and adapt their methods to circumvent existing countermeasures.[506] Overall, stakeholders anticipate that the increasing use of AI agents in the execution of scams is likely to become a significant future trend.[507]

The use of operational tools and AI is complemented by behavioural manipulation techniques, which target heuristics and psychological vulnerabilities in potential victims, as described below.

3.2.5. Social engineering methods

In addition to technical tools, fraudsters heavily rely on social engineering techniques designed to manipulate victims psychologically, induce a state of vulnerability, and lower vigilance. A key enabling condition is the **documented gap between consumers' confidence in their ability to identify scams and their actual performance** when tested.[508] This 'overconfidence gap' can be exploited by offenders: individuals who believe they are unlikely to be deceived may, paradoxically, engage with suspicious offers for longer or apply fewer verification steps when confronted with a well-constructed scheme.

[502] Interview 8.

[503] Interview 1.

[504] Pava et al., Mind the (Language) Gap: Mapping the Challenges of LLM Development in Low-Resource Language Contexts (2025), available at: https://hai.stanford.edu/policy/mind-the-language-gap-mapping-the-challenges-of-llm-development-in-low-resource-language-contexts

[505] Interviews 1, 7.

[506] Interviews 1, 7, 11.

[507] Interviews 11, 15.

[508] Verbraucherzentrale Bundesverband, Bank Oder Betrüger? Erhebung zur Erkennbarkeit von Betrug im digitalen Zahlungsverkehr (2024), available at: https://www.vzbv.de/sites/default/files/2024-05/24-05-09%20Bericht_vzbv_Betrugserkennung.pdf

More broadly, research on the psychology of scam victimisation suggests that scams are most effective when **victims are pushed beyond their emotional 'window of tolerance', that is, into states of cognitive and emotional overload in which normal critical faculties are compromised**.[509] The behavioural techniques described below (emotional manipulation, urgency tactics, fabricated emergencies, and the management of relationship intimacy) function precisely by shifting victims into a reactive state. Stakeholder interviews similarly emphasise manipulation tactics such as instilling fear, creating urgency, and targeting individuals at vulnerable moments as recurring features across scam types.[510]

The most sustained and structurally sophisticated behavioural model is **staged trust-building**: the deliberate, slow-paced construction of a relationship of confidence before any financial request is made.[511] This model is most visible in romance scams, where offenders invest weeks or months in establishing emotional rapport, often presenting themselves as romantic partners, peers, or successful acquaintances with specialised financial knowledge. Initial contact is typically framed as incidental or casual (e.g. a 'wrong number' approach), after which continuous interaction gradually normalises intimacy and dependence; only once trust is established is the investment or transfer request introduced, with the victim's relationship-based trust lowering their critical evaluation of the 'opportunity'.[512]

Importantly, trust-building is not limited to romance-based schemes. Investment scams increasingly blend short- and longer-term trust-building strategies, often using group dynamics to simulate transparency and insider access.[513] 'Exclusive tip' groups on messaging apps can create a sense of community, repeated exposure, and social validation, which can make the investment narrative feel less like a solicitation and more like participation in a knowledgeable peer network.[514] A structurally similar pattern can be observed in rental and accommodation scams: fraudsters mimic genuine host or landlord communication styles, provide responsive, detailed messaging, and use apparent reasonableness or appeals to sympathy to quickly build credibility by replicating the same grooming logic, but without the romantic component.[515]

A second cluster of social engineering techniques relies on **urgency and scarcity signals ('sale ends today', 'only available today', 'sells out fast') to compress decision-making time and prevent scepticism from developing**. This mechanism is central to many e-commerce and non-delivery scams, where implausibly low prices are paired with time-limited

[509] Which?, The psychology of scams, Understanding why consumers fall for APP scams (2022), available at: https://media.product.which.co.uk/prod/files/file/gm-c66f3d70-3928-4dee-bb8b-481405be2b5e-the-psychology-of-scams-understanding-why-consumers-fall-for-app-scams.pdf.

[510] Interviews 1, 3, 4, 7.

[511] Cassandra Cross and Karen Holt, To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581; Rajvardhan Oak and Zubair Shafiq, "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf.

[512] ibid.

[513] Matthew Anderson et al., Exploring the roles played by trust and technology in the online investment fraud victimisation process (2024) available at: https://journals.sagepub.com/doi/pdf/10.1177/26338076241248176.

[514] Interview 5; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[515] Malwarebytes, Booking.com breach gives scammers what they need to target guests (2026), available at: https://www.malwarebytes.com/blog/data-breaches/2026/04/booking-com-breach-gives-scammers-what-they-need-to-target-guests

framing to suppress careful evaluation of the site's legitimacy. Consistent with this logic, scam activity often intensifies around periods of peak consumer spending (e.g., Black Friday and holiday shopping periods), when users are already primed to act quickly and may be less attentive to verification cues.[516]

Artificial time pressure also appears through the exploitation of instant payment systems. Fraudsters leverage the speed and irreversibility of instant payments precisely because they leave less time for reflection or bank-side intervention.[517] The convenience of instant payments, while beneficial for consumers in legitimate contexts, is thus weaponised as a structural component of the scam model. The Instant Payments Regulation aims to make instant money transfers safer by introducing additional safeguards, such as payee name verification or daily screening by payment service providers of customers against sanctions lists.[518] However, as the regulation partially entered into force in October 2025, no data is available yet as to the effectiveness of these new measures.

Another major cluster of psychological techniques operates through the **invocation of authority and institutional legitimacy.** Fraudsters impersonating tax agencies, financial regulators, law enforcement bodies, or other public institutions exploit the deference and anxiety associated with official communications, particularly where penalties, liabilities, or compliance failures are implied.[519] A closely related mechanism is the **impersonation of trusted private institutions** such as banks, insurers, lenders, or investment platforms, designed to trigger automatic trust in regulated brands and familiar administrative processes.[520]

Even where the victim does not explicitly trust the message sender, the presence of **'recognised' authority markers (logos, credentials, platform-like interfaces, purported expert endorsements) can reduce suspicion and make the scam feel more legitimate.**

Many scams exploit victims' **pre-existing financial vulnerability as an entry point**. Loan and credit scams promise fast, unconditional access to funds without credit checks, targeting individuals already in precarious circumstances.[521] Related 'easy money' framings also appear in investment and fake job scams, where participation is presented as a plausible route out of

[516] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[517] Interview 7; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[518] European Central Bank, Instant Payments Regulation, available at: https://www.ecb.europa.eu/paym/retail/instant_payments/html/instant_payments_regulation.en.html.

[519] Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/.

[520] Financial Services and Market Authority, Cloned firms: theft of the identity of authorized companies, available at: https://www.fsma.be/en/cloned-firms-theft-identity-authorized-companies.

[521] Interview 5; see also L'Autorité de contrôle prudentiel et de résolution (ACPR), L'ACPR met en garde le public contre la multiplication de fausses offres de prêt immobilier ou de rachat de crédit proposées par des individus usurpant l'identité de courtiers et d'établissements de crédit (2024), available at: https://acpr.banque-france.fr/fr/communiques-de-presse/lacpr-met-en-garde-le-public-contre-la-multiplication-de-fausses-offres-de-pret-immobilier-ou-de.

hardship.[522] Offenders aim to present the scam as a solution to immediate pressure, leveraging an emotional response.

By contrast, charity scams and fraudulent crowdfunding campaigns typically operate through prosocial motivation rather than self-interest. Fraudsters construct emotionally engaging narratives around humanitarian crises, disasters, or personal hardship, using vivid imagery and stories to activate empathy and moral obligation.[523]

Access to the operational tools and behavioural methods described in the previous sections is facilitated through black markets which commercialise scam toolkits. These are briefly presented in the following section.

3.2.6. Fraud-as-a-service infrastructure

Adjacent to the operationalisation of online financial scams, reports increasingly highlight the emergence of **'fraud-as-a-service' (FaaS) markets, through which ready-to-use tools, infrastructure and expertise are sold for the operation of online financial scams**.[524] FaaS functions as an industrialisation of cybercrime, significantly lowering the barrier to entry for malicious actors, enabling the deployment of complex fraud campaigns and accelerating their impact.[525] The consequence of this structural development is that any actor willing to pay can access the operational tools (e.g., deepfake generation, phishing templates, website creation or cloning infrastructure, bot scripts) required to implement a financial scam, which would have previously required significant criminal expertise. Specific manifestations of this model, including phishing-as-a-service, cloaking-as-a-service, and spoofing-as-a-service, are discussed in Section 3.2.3 above.

The takedown of the LabHost platform in April 2024, coordinated by Europol across 19 countries, provides the most detailed documented illustration of the FaaS model in operation. For a monthly subscription averaging $249, LabHost provided phishing kits, infrastructure for hosting pages, interactive functionality for directly engaging with victims, and campaign overview services. Depending on the subscription tier, criminals were offered an escalating scope of targets, ranging from financial institutions to postal delivery services and

[522] Interview 7.

[523] Europol, Online fraud schemes – A web of deceit (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/e914d7fe-b429-11ee-b164-01aa75ed71a1/language-en; Seunghun Lee et al., Fraud Detection on Crowdfunding Platforms Using Multiple Feature Selection Methods (2025), available at: https://xplorestaging.ieee.org/ielx8/6287639/10820123/10909102.pdf?arnumber=10909102&utm_source=scopus&getft_integrator=scopus

[524] Interview 2; see also Europol, Internet Organised Crime Threat Assessment 2025 (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf; Europol, Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en.

[525] Juniper Research, Fraud-as-a-Service: Inside the Dark Web's Booming Business Model (2024), available at: https://www.juniperresearch.com/resources/blog/fraud-as-a-service-inside-the-dark-webs-booming-business-model/.

telecommunications providers.[526] These types of services are typically accessed through online environments including specialised forums, dark web marketplaces, and encrypted messaging platforms.[527] Despite some evidence of FaaS services being occasionally accessible on the open web, the majority of activity seems to take place on the dark web instead.[528]

The FaaS model has important implications for the threat landscape described in this report. It means that the **technical sophistication of individual attacks cannot be used as an indicator of the technical sophistication of the actors behind them: a highly convincing deepfake advertisement or a cloned investment platform may have been assembled by a non-technical actor using off-the-shelf tools.**

Beyond FaaS infrastructure, online financial scams are increasingly operated by **organised cybercrime networks with transnational reach.** These networks are often based in jurisdictions with weak regulatory frameworks, enabling them to exploit legal loopholes and jurisdictional barriers. Organised crime groups have been identified in East and Southeast Asia, West Africa, Eastern Europe, the Middle East, and Latin America, sometimes operating in cooperation with one another.[529] Of particular concern are large-scale scam operations conducted from purpose-built compounds, often located in border regions with limited governance or within special economic zones.[530] Such compounds have been described as functioning similarly to commercial enterprises, with hierarchical management structures, specialised teams, performance targets, and clearly defined divisions of labour.[531] Individuals involved in these operations do not necessarily participate voluntarily; evidence indicates that some are recruited through deceptive job advertisements and subsequently subjected to coercion, debt bondage, or other forms of exploitation, including physical violence, threats,

[526] Europol, International investigation disrupts phishing-as-a-service platform LabHost (2024), available at: https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost.

[527] ITPro, 'Phishing kits are a force multiplier': Cheap cyber crime kits can be bought on the dark web for less than $25 – and experts warn it's lowering the barrier of entry for amateur hackers (2025), available at: https://www.itpro.com/security/cyber-attacks/phishing-kits-cyber-crime-dark-web.

[528] Europol, International investigation disrupts phishing-as-a-service platform Labhost (2024). available at: https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost; Thomas Wilson, Fraud-as-a-Service: Inside the Dark Web's Booming Business Model (2024), available at: https://www.juniperresearch.com/resources/blog/fraud-as-a-service-inside-the-dark-webs-booming-business-model/.

[529] Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/; Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en.

[530] Office of the United Nations High Commissioner for Human Rights (OHCHR), Hundreds of Thousands Trafficked into Online Criminality in Southeast Asia (2023), available at: https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report; Fondation pour la Recherche Stratégique (FRS), Scam Centers in the Mekong Region: A Strategic Challenge for the European Union (2026), available at: https://www.frstrategie.org/en/publications/notes/scam-centers-mekong-region-strategic-challenge-european-union-2026.

[531] ibid.

confinement, and torture.[532] Since 2020, more than 200,000 people may have been trafficked to work as online scammers, from 66 countries across continents.[533] This intersection of online financial scams with human trafficking represents a distinct dimension of the threat landscape.

[532] United Nations News, Global Scam Centres Expand Rapidly, Threatening Millions Worldwide (2026), available at: https://news.un.org/en/story/2026/02/1167012.

[533] Interpol, INTERPOL Releases New Information on Globalization of Scam Centres (2025), available at: https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres.

4. Social and economic impact of online financial scams

Building on the previous sections, the following paragraphs shift attention to the victims of online financial scams, assessing the impact of each scam type and expanding the findings into a generalised picture of the harms associated with online financial scams.

As a primer to the detailed assessment of victimology and impact, the following table presents **a consolidated overview of available prevalence and economic impact data by scam type.** Figures on social impact are not included, as this type of harm could not be quantified.

Readers should note that **data availability, methodology, and geographic scope vary significantly across scam types**. For that reason, some scam types or categories were not included, as no relevant data were available. Where EU-level data is unavailable, national figures and enforcement-derived estimates are provided. Data limitations are flagged for each category to assist the reader in assessing the reliability and comparability of the figures presented.

Table 4 - Overview of prevalence and economic impact

Scam Type	Victimisation Rate / Exposure	Estimated Losses (EU / National)	Data Limitations
Investment Scams (Traditional)	25–40% across EU Member States (GASA 2025): NL 25%, DE 34%, ES 35%, FR/IT 36%, BE 40%	EUR 4 billion in Europe (2024); EUR 120 million in Austria	Reported cases only; true scale likely significantly underestimated (~15% reporting rate)
Cryptocurrency Scams	Subset of investment scams; no separate victimisation rate available	Global: EUR 15 billion (2025 est.); Belgium: EUR 10.5 million	Predominantly global figures; attribution to EU Member States challenging
Romance Scams	27–37% across EU (GASA 2025): ES 27%, NL/IT 28%, DK 30%, FR 34%, BE 36%, DE 37%	Sweden: EUR 50 million; Netherlands: EUR 7.6 million (avg. ~EUR 29,000/victim)	Significant under-reporting due to stigma; figures vary considerably by country
Non-delivery Scams	High volume; most frequently reported scam type across several Member States	Netherlands avg.: EUR 350/victim; BogusBazaar network: EUR 43 million (2021–2024)	High volume but lower individual losses; aggregate EU figures not available

Scam Type	Victimisation Rate / Exposure	Estimated Losses (EU / National)	Data Limitations
Health and Wellness Scams	Systematic data limited; prevalence not separately measured in surveys	EUR 11.1 million in seizures (Europol Operation SHIELD V)	EU-wide prevalence data not available; enforcement data only
Event Ticket Scams	Systematic data limited; spike around major sporting/cultural events	UK: EUR 11 million (2024); Belgium avg.: EUR 168/victim	National-level data only; no EU-wide aggregation
Loan / Credit Scams	Systematic data limited; prevalence not separately measured	France: EUR 19,000/victim (2024)	National data only; significant under-reporting likely
Rental Scams	Systematic data limited; concentrated in high-demand urban housing markets.	EUR 200–10,000/victim (Europol case data)	Case-based evidence only; no systematic EU data collection
Fake Job Scams	Systematic data limited; growing prevalence noted by Europol	US: EUR 227 million (2024); no comparable EU figure	No EU-level data available; US figures not directly transferable
Charity Scams	34% of UK charities reported fraud attempts (2025)	UK: EUR ~ 13,000 – 128,000 per affected charity	Primarily UK data; EU-wide prevalence and loss estimates not available

Against this background, the following sections explore the types of victims behind these numbers and the harms associated with their victimisation.

4.1. Victims of online financial scams

As a general disclaimer, it is important to note that anyone can become a victim of online financial scams, regardless of age, background, or level of experience.[534] The scale of victimisation remains difficult to quantify precisely due to significant under-reporting, meaning that available figures are estimates. Victimisation figures come either from official criminality statistics of law enforcement authorities, or from self-reported surveys. One interviewee **estimated that only 15% of victims report the crime**.[535] The figures presented below should therefore be understood as indicative rather than exhaustive.

[534] Interviews 4, 5, 7, 9.

[535] Interview 1.

4.1.1. General patterns of victimisation

At the global level, survey data from the Global Anti-Scam Alliance (GASA) indicate that in 2024, 57% of adults claim to have encountered a scam, whether successfully scammed or not.[536] Other global estimates from the Financial Action Task Force suggest that up to 15% of the adult population have experienced at least one successful cyber-enabled scam attempt.[537] A 2021 survey by the European Union Agency for Fundamental Rights (EU FRA) reports that one in four people (26%) in the EU27 experienced an incident of consumer fraud[538] in the five years before the survey, and 16% in the 12 months before the survey.[539] The rates of consumer scams vary from 46% (Estonia) to 8% (Cyprus), depending on the country.[540]

A more recent consumer survey by EU FRA found that **one in four people in the EU fell victim to online scams in their lifetime**.[541] Among those who experienced one or more instances of online scams, over one in three (37%) fell victim to more than one type of scam in their lifetime.[542] According to the Consumer Conditions survey, in 2024, more than 4 in 10 European consumers (45%) encountered fraudulent practices online.[543] The most frequent were fake requests for money to alleviate financial hardship (23%) and phishing for personal information (21%).[544] Moreover, ENISA data from 2024 indicate that, overall, phishing campaigns affected 38% of European individuals in 2024.[545] For payment fraud, survey data from a 10-EU country assessment indicates that 22% of adults and 18% of teenagers have experienced payment scams or security breaches over five years.[546]

---

[536] GASA, Global State of Scams (2025), available at: https://gasa.org/knowledge-base/reports/global-state-of-scams-2025

[537] FATF, Cyber-enabled fraud (2026), available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/cyber-enabled-fraud-digitalisation-ml-tf-pf-risks.html

[538] This involves feeling cheated or misled in terms of quantity, quality, pricing or delivery of goods, items or services purchased.

[539] European Union Agency for Fundamental Rights, Crime, safety and victims' rights (2021), available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-crime-safety-victims-rights_en.pdf.

[540] ibid.

[541] European Union Agency for Fundamental Rights, Online Fraud – People's experiences across the EU (2026), available at: https://fra.europa.eu/en/publication/2026/victims-online-fraud.

[542] ibid.

[543] European Commission, 2024 Consumer conditions survey – Full data set (2025), available at: https://commission.europa.eu/publications/2024-consumer-conditions-survey-full-data-set_en.

[544] ibid.

[545] ENISA, Threat Landscape 2024 (2024), available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[546] BEUC, Free, easy and secure – What consumers expect from the digital euro (2025), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-085_What_consumers_expect_from_the_digital_euro-copy.pdf; The 10 countries are Italy, Austria, Spain, Netherlands, Portugal, Greece, Belgium, France, Germany, Slovenia.

Overall patterns of victimisation indicate that **scammers frequently target individuals rather than organisations or private sector entities** and predominantly aim at victims who are perceived as **inexperienced online users**.[547] This group includes both older adults and very young people, whose understanding of online security may be limited.[548] More broadly, people with low media literacy and those around 55-60 years of age are often identified as primary targets, as they may be less able to recognise fraudulent schemes.[549] At the same time, the profile of victims is constantly evolving. Scams increasingly target younger individuals, in part due to the widespread use of social media. Younger individuals are highly present in digital environments and tend to display confidence online, which may lead to significant sharing of personal information and increased exposure to fraud.[550] Further, people who are limited in their usual activities (by health problems or disability) are also more exposed than those who do not have such limitations. Higher exposure is also associated with belonging to an ethnic minority and self-identifying as lesbian, gay, bisexual or 'other'.[551]

At the European level, data indicate that more frequent internet users, individuals with higher levels of education, and those aged between 34 and 54 years are more likely to experience online scams.[552] Specifically, the probability of experiencing scams goes up by 25 percentage points for someone who uses the internet at least once a week compared to someone who rarely uses it.[553] Higher education is associated with a 7-percentage-point increase in the likelihood of being scammed, while those in very difficult financial situations are 5 percentage points less likely to experience scams compared to those who are financially comfortable.[554] Based on a survey from 2025 of more than 7,000 consumers across the US, UK, France, Germany, Spain, Italy, and Australia, the highest shares of respondents reporting that they had fallen victim to a scam in the last 12 months were among young people: 19.8% of 16-24 years old, 19.9% of 25-35 years old, compared to 11.7% of 45-54 and 9.7% of 55+ years old.[555]

---

[547] Interpol, Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf

[548] Interview 1.

[549] Interviews 2, 6; Multi-stakeholder Workshop on Online Financial Scams.

[550] Interview 7.

[551] European Union Agency for Fundamental Rights, Crime, safety and victims' rights (2021), available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-crime-safety-victims-rights_en.pdf

[552] European Commission, Survey on "Scams and Fraud Experienced by Consumers", Final Report (2020), available at: https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

[553] ibid.

[554] GASA, Global State of Scams (2025), available at: https://gasa.org/knowledge-base/reports/global-state-of-scams-2025; ibid.

[555] Bitdefender, Consumer cybersecurity survey (2025), available at: https://blogapp.bitdefender.com/hotforsecurity/content/files/2025/11/11052025-2025-Consumer-Cybersecurity-Survey.pdf?_gl=1*u3fy9f*_gcl_au*NTc3OTk2MDAuMTc3Mjc4NTc3Mg..*_ga*Mzk2NTc3OTU5LjE3NzI3ODU3NzI.*_ga_6M0GWNLLWF*czE3NzI3ODU3NzAkbzEkZzAkdDE3NzI3ODU3NzAkajYwJGwwJGgzODM0ODQwNjQ

Although individuals from all EU Member States are highly exposed to scams, some variations between countries exist. According to the Consumer Conditions survey, in 2024, there was wide variation in the exposure of fraudulent practices online by country, ranging from less than a third of consumers having encountered fraudulent activities in Finland (29%), to more than four in five in Austria (85%), while the average of the EU27 lies at 40%.[556] A 2022 study based on Eurobarometer data further estimated that, among individuals aged 15 and above in the EU 27, approximately 10 million had experienced identity theft or impersonation, 113 million had been affected by phishing, and 88 million had encountered malware.[557]

In France, online payment-related scams account for half of all cases in 2024 (50%), up from 31% in 2016.[558] More than half of French people (57%) say they have already been the target of an attempt to steal their bank details, while 13% report having been scammed, representing a 5% increase compared to the previous year.[559] French young adults are disproportionately affected, with the highest victimisation rate among those aged 20-24, and individuals aged 18-44 account for nearly 45% of victims despite representing a smaller share of the population.[560] The reporting platform Thésée, launched in 2022, indicates that 53,300 complaints were filed in 2024, representing 11% of all recorded victims, a decrease from 14% in 2023.[561]

In Spain, the number of registered online scam cases rose rapidly from 257,907 in 2020 to 427,448 in 2023, before declining slightly to 412,850 in 2024.[562] Over a longer period, cyber-related scams have grown significantly, now accounting for 18% of all criminal offences in 2025, with a 490% increase between 2016 and 2024.[563] More than 70% of the population has been targeted by a scam within six months.[564]

---

[556] European Commission, Consumer Conditions Scoreboard (2025), available at: https://commission.europa.eu/document/download/2816337b-4fd1-4db2-a71c-d14a206a5a93_en?filename=consumer_conditions_scoreboard_2025_final.pdf

[557] European Commission, Study on online identity theft and identity related crime – Final report (2022), available at: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1/language-en

[558] FBF, Perceptions et comportements des français en matière de cybersécurité – Etude Harris Interactive 2024 (2024), available at: https://www.fbf.fr/fr/etude-2024-sur-les-perceptions-et-comportements-des-francais-en-matiere-de-cybersecurite/ç

[559] ibid.

[560] ibid.

[561] OSMP, Rapport de l'Observatoire de la sécurité des moyens de paiement 2024 (2024), available at: https://www.banque-3france.fr/fr/publications-et-statistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2024

[562] OCC, Informe sobre la cibercriminalidad en España (2024), available at: https://occ.ses.mir.es/publico/occ/dam/jcr:b9a4f43b-88c7-48f9-ab12-9b6891288b4c/Informe-sobre-la-cibercriminalidad-en-Espa%C3%B1a-2024.pdf.

[563] ibid.

[564] Levanta la cabeza, El fraude digital aumenta un 40% en España: 1.200 estafas al día en 2025 (2025), available at: https://www.atresmedia.com/levanta-la-cabeza/buenas-practicas/ciberseguridad/fraude-digital-aumenta-40-espana-1200-estafas-dia-2025_202512306953a7ee22f0db7daf011949.html; OCC, Informe sobre la cibercriminalidad en España (2024), available at:

In Belgium, more than half of the population reported receiving at least one phishing message in 2023, with 8% falling victim to this type of scam; the number of victims rose to 13% in 2024.[565]

Additional data from GASA on victims of online financial scams by country is depicted in the table below. The highest rate of individuals who reported having been scammed was recorded in the Netherlands (56%), and the lowest share was noted in Sweden (37%).

Table 5 - Survey data on scam victimisation in 2025 from the Global Anti-Scam Alliance[566]

	France	Germany	Belgium	Sweden	Netherlands
Individuals who reported having encountered a scam	63%	54%	65%	57%	74%
Individuals who reported having been scammed	54%	46%	55%	37%	56%

4.1.2. Scam-specific patterns of victimisation

While exposure to scams is widespread, **certain types of scams disproportionately target specific population groups,** as one interviewee indicated.[567] The following sections outline the characteristics of victims by scam type. Please note that data is not

https://occ.ses.mir.es/publico/occ/dam/jcr:b9a4f43b-88c7-48f9-ab12-9b6891288b4c/Informe-sobre-la-cibercriminalidad-en-Espa%C3%B1a-2024.pdf

[565] Febelfin, Phishing & austres arnaques en vue (2024), available at: https://febelfin.be/media/pages/publicaties/2024/phishing-en-andere-kapers-op-de-kust/48633be3fd-1718872012/storytelling_phishing_fr_final.pdf; Febelfin, Chiffres 2024: 'Si ça ressemble à du phishing, c'est probablement du phishing !' (2025), available at: https://febelfin.be/fr/themes/fraude-et-securite/chiffres-et-tendances/chiffres-2024-si-ca-ressemble-a-du-phishing-c-est-probablement-du-phishing

[566] GASA, State of Scams in the Netherlands (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_e4b2335bcebd496cab156f9a2440b6e1.pdf; GASA, State of Scams in Italy (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_90a4ada9f8be41b3b601995d679f5d30.pdf; GASA, State of Scams in Spain (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_737deba33aa546088296efc5ab7dff26.pdf; GASA, State of Scams in Germany (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_dbef245762ef487797354a803b67eb14.pdf; GASA, State of Scams in Denmark (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_3333c506a2274110988e0092bb9b04d4.pdf; GASA, State of Scams in Belgium (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_f4d15a699656439fb4ebfb9a5bdd55a1.pdf; GASA, State of Scams in France (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_fa620227910a4e8ebc06c0cd5e036614.pdf.

[567] Interview 4.

available for all scam types included in the typology. Therefore, only those for which data is available are discussed below.

Investment scams

Traditional investment scams

According to an online self-selected response survey led by GASA in 2025, investment scams were reported by 25% of respondents in the Netherlands, 34% in Germany, 35% in Spain, 36% in both France and Italy, reaching 40% in Belgium.[568] In Austria, Watchlist Internet estimates that advertisements for fraudulent investment platforms have reached approximately 200,000 individuals every day.[569] Survey data from France indicates that 3.2% of the population fell victim to investment scams in 2024, a proportion that has nearly tripled since 2021.[570]

At the individual level, investment scams have traditionally targeted older individuals as increasing numbers of retirees manage their retirement/redundancy assets and may therefore be more exposed to fraudulent offers promising unrealistic returns.[571] Individuals with higher incomes and higher levels of education may also be targeted. Higher risk tolerance, engagement in speculative behaviour, and higher levels of debt are further associated with an increased likelihood of victimisation.[572] However, younger individuals are also targeted, particularly through social media content designed to encourage viral sharing and appeal to users with limited investment experience.[573]

---

[568] Global Anti-Scam Alliance, State of Scams in The Netherlands – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_e4b2335bcebd496cab156f9a2440b6e1.pdf; Global Anti-Scam Alliance, State of Scams in Germany – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_dbef245762ef487797354a803b67eb14.pdf; Global Anti-Scam Alliance, State of Scams in Spain – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_737deba33aa546088296efc5ab7dff26.pdf; Global Anti-Scam Alliance, State of Scams in France – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_fa620227910a4e8ebc06c0cd5e036614.pdf; Global Anti-Scam Alliance, State of Scams in Italy – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_90a4ada9f8be41b3b601995d679f5d30.pdf; Global Anti-Scam Alliance, State of Scams in Belgium – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_f4d15a699656439fb4ebfb9a5bdd55a1.pdf.

[569] Watchlist Internet, Promis als Lockvögel: Werbung für betrügerische Investmentplattformen erreicht täglich 200.000 Österreicher:innen (2024), available at: https://www.watchlist-internet.at/news/werbung-promis-investmentbetrug/.

[570] Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes, Arnaques financières : les autorités mobilisées dans la lutte contre ce phénomène massif qui piège de plus en plus de particuliers (2024), available at: https://www.economie.gouv.fr/files/files/directions_services/dgccrf/media-document/cp-dgccrf-conference-afm.pdf.

[571] Marguerite DeLiema, Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors (2019), available at: https://academic.oup.com/jcr/article-abstract/46/5/904/5512363.

[572] Christine N Kieffer and Gary R Mottola, Understanding and Combating Investment Fraud (2016), available at: https://pensionresearchcouncil.wharton.upenn.edu/wp-content/uploads/2017/02/WP2016-19-Kieffer-and-Mottola.pdf.

[573] Interview 4 ; Autorité des Marchés Financiers, Social Media Intelligence: Arnaques à l'investissement sur le web (2024), available at: https://www.amf-france.org/sites/institutionnel/files/private/2024-

Factors such as overconfidence, perceived financial knowledge, and a willingness to take risks may increase vulnerability.

Although victims of investment scams are predominantly individuals, companies may also be affected.[574] According to the UK Economic Crime Survey, in 2024, 22% of businesses (from the 3,477 businesses with employees surveyed) had experienced investment scams, with finance and insurance businesses more likely to see themselves as being at risk from scams (24% versus 15% overall).[575] A typical type of scam that businesses face is Business Email Compromise (BEC), including CEO fraud, where criminals impersonate senior company executives for malicious purposes. Offenders often obtain credentials through phishing techniques such as spear-phishing and whaling, which may be disseminated via online platforms, advertising systems, or messaging services operated by the designated services.[576]

Cryptocurrency scams

While traditional investment scams affect pensioners or people close to retirement age, cryptocurrency scams typically have a more youthful target, appealing to the younger population who are more drawn to the factors of risk and speed, and to the promise of an easy way to gain money.[577] A recently dismantled cryptocurrency Ponzi scheme by Belgian and Swiss law enforcement authorities suggests that 223,000 individuals from 177 countries have fallen victim to this scheme.[578]

Romance scams

Traditional romance scams

12/opinionway-pour-amf-les-arnaques-sur-le-web_octobre-2024_0.pdf; See also Faux, Zeke, *Number go up: Inside Crypto's wild rise and staggering fall* (2024, Penguin Random House).

[574] Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en;

[575] UK Home Office, Economic Crime Survey (2025), available at: https://www.gov.uk/government/publications/economic-crime-survey-2024/economic-crime-survey-2024.

[576] European Commission, Study on online identity theft and identity related crime – Final report (2022), available at: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1/language-en

[577] Interview 4; see also Faux, Zeke, *Number go up: Inside Crypto's wild rise and staggering fall* (2024, Penguin Random House); BaFin, Investitionen in Kryptowerte und der Einfluss sozialer Medien auf das Anlageverhalten (2026), available at: https://www.bafin.de/DE/Aufsicht/Fokusrisiken/Fokusrisiken_2026/RIF_verbraucher_sozialemedien/RIF_verbraucher_sozialemedien_node.html;jsessionid=7482B626CD4BA5A50D21116827D3E0A2.internet012

[578] Europol, Europol Spotlight - Cryptocurrencies: tracing the evolution of criminal finances (2022), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Identifying a consistent victim profile for romance scams remains challenging, as vulnerability cuts across demographic and socio-economic groups.[579] Nevertheless, overall, lonely people seeking emotional connection fall prey more easily to romance scams, as they crave contact with other individuals.[580] Victims are relatively well educated and may display behavioural traits such as impulsivity, lower self-control and a higher propensity to trust.[581] Other factors associated with vulnerability include limited digital skills and social circumstances, such as experiencing isolation or seeking companionship.[582] Young people and students are often identified as victims, while individuals experiencing loneliness or emotional distress may also be more susceptible.[583] In the case of sextortion, children and particularly boys are identified as victims.[584] Single women aged 35 to 54 with higher levels of education and disposable income appear to be particularly exposed, partly due to higher engagement with online dating platforms.[585] At the same time, older individuals aged 55 years and above are also likely to be targeted.[586] Data from the United States indicate that nearly half of reported victims of online dating scams fall within the 50-59 and 60+ age groups.[587] In parallel, increasing numbers of younger men are also affected.[588] Interestingly, data from Denmark suggests that men are more likely to be victims than women (4% of Danish men have been exposed to romance scams compared to 1% of women in 2025).[589]

[579] Cassandra Cross and Karen Holt, To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581.

[580] Interview 1.

[581] Monica Whitty, Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims (2020), available at: https://link.springer.com/article/10.1007/s10610-020-09458-z; Cassandra Cross and Karen Holt, To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581.

[582] Mohd Ezri Saad, Cyber Romance Scam Victimization Analysis using Routine Activity Theory Versus Apriori Algorithm (2018), available at: https://www.proquest.com/openview/8b75a9c1d7acab599b654754d2482c26/1?pq-origsite=gscholar&cbl=5444811; Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en

[583] Interview 1.

[584] European Union, Better Internet for Kids – Sextortion, available at: https://better-internet-for-kids.europa.eu/en/learning-corner/teachers-and-educators/sextortion.

[585] Monica Whitty, Do You Love Me? Psychological Characteristics of Romance Scam Victims (2018), available at: https://journals.sagepub.com/doi/full/10.1089/cyber.2016.0729.

[586] Interview 6.

[587] Drew & Webster, The victimology of online fraud: A focus on romance fraud victimisation (2024), available at: https://www.sciencedirect.com/science/article/pii/S2949791424000058

[588] Alexander Bilz et al., Tainted Love: a Systematic Literature Review of Online Romance Scam Research (2023), available at: https://academic.oup.com/iwc/article/35/6/773/7331428.

[589] Taenk, Digital svindel i Danmark - En undersøgelse af danskernes holdninger, erfaringer og adfærd (2025), available at: https://taenk.dk/system/files?file=2025-05/Digital%20svindel%20i%20Danmark_FINAL_290425.pdf

Romance baiting

Romance baiting does not show a pronounced age skew in the literature. Instead, victims are often defined more by situational drivers such as financial aspirations and interest in cryptocurrency markets.[590]. One piece of evidence suggests that individuals aged 25 to 34 are particularly affected, especially those with higher levels of education and familiarity with digital technologies.[591]

E-commerce scams

Subscription scams and hidden renewals

In 2017, it was reported that 3.5 million European consumers were estimated to have been affected by subscription scams over the preceding three years.[592] A study from 2020 further states that 8% of EU consumers surveyed experienced some form of subscription scam.[593]

Artificial streaming scams

Artificial streaming scams primarily harm advertisers and content creators, as viewbotting distorts performance metrics, misleading brands and negatively affecting the reach of paid advertisements.[594] As such, ad placements, which are designed to reach real humans, are in practice shown to inauthentic accounts, jeopardising their promotional objective and potentially hampering the ability of brands to market their products.

Insurance scams

While all categories of users may fall victim to this type of scam, young adults are more likely to be victimised, as they tend to use social media platforms more to search for insurance deals. In the UK, reports found that one in five adults aged 18-24 has used social media to this end.[595] Although comparable data at EU level is not available,

[590] Fangzhou Wang, A scoping review of online romance scams: Conceptual construction and comparative analysis (2026), available at: https://journals.sagepub.com/doi/pdf/10.1177/02697580251414141.

[591] Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670.

[592] Hietanen, Crime Prevention – How to Avoid Subscription Traps (2018), available at: https://apfjournal.or.id/index.php/apf/article/view/79/92

[593] European Commission, Survey on 'Scams and Fraud Experiences by Consumers' (2020), available at: https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf; European Commission, Commission Staff Working Document on EU Consumer Law on Digital Fairness (2024), available at: https://commission.europa.eu/document/707d7404-78e5-4aef-acfa-82b4cf639f55_en.

[594] StreamCharts, The Hidden Cost of Viewbotting (2025), available at: https://streamscharts.com/reports/viewbotting-whitepaper; Andrew Chu et al., Behind the Tube: Exploitative Monetization of Content on YouTube (2022), available at: https://www.usenix.org/system/files/sec22-chu.pdf/.

[595] Insurance Fraud Bureau, Don't be caught out by fake car insurance - The Result Could Be Crushing, available at: https://www.insurancefraudbureau.org/en/ghost-broking.

evidence from European national authorities indicates that similar practices affect European citizens as well.[596]

Loan and credit offer scams

Victims of loan and credit offer scams are typically individuals who are already in a financially precarious situation, making the impact of this scam particularly severe. In fact, some stakeholders have noted that this type of scam follows a sort of cyclical scheme, as they are most prominent in those periods of the year when consumers are encouraged to spend and are on the lookout for more funds: Black Friday, before Christmas, and at the start of the school year.[597]

Rental scams

Victims of rental scams are frequently individuals who are logistically unable to inspect a property before committing to it. In the context of longer-term rentals, this includes students and people relocating across cities or countries, who face practical and financial barriers to in-person viewings.[598] For vacation rentals, victims are typically travellers based in a different country, again with no realistic means of verifying the legitimacy of a listing prior to their arrival. Scammers tend to rely on the popularity of a given travel destination. In fact, vacation rental scams are more popular not only in particular periods, i.e. the summer months, but also in specific, highly sought-after areas.[599] These groups are more prone to being victimised through fake listings – however, all users of accommodation rental platforms may be exposed to phishing scams carried out through business accounts active on the platform that were hijacked by scammers.

Employment and collaboration scams

Fake job scams

Preliminary research suggests that victims of fake job scams are often individuals experiencing unemployment or seeking to switch from part-time employment to full-time.[600] However, this correlation requires further investigation to be validated. Ofcom reports that 30% of adult victims of online scams in the UK have experienced a fake employment scam.[601] In Europe, an investigation from Euronews found that thousands of people have been targeted on WhatsApp in the context of a fake employment scam,

[596] FSMA (2025)

[597] Interview 4; Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[598] Sophie Van Der Zee et al., The gift of the gab: Are rental scammers skilled at the art of persuasion? (2019), available at: https://arxiv.org/abs/1911.08253.

[599] Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[600] Christina Policastro and Brian K Payne, Can you hear me now? Telemarketing fraud victimisation and lifestyles’ (2015), available at: https://www.researchgate.net/publication/280973645_Can_You_Hear_Me_Now_Telemarketing_Fraud_Victimization_and_Lifestyles.

[601] Ofcom, Scale and impact of online fraud revealed (2023), available at: https://www.ofcom.org.uk/online-safety/online-fraud/scale-and-impact-of-online-fraud-revealed.

which is estimated to have caused more than EUR 100 million in financial losses.[602] Concurrently, US figures estimate that 20-40% of job postings are ghost jobs.[603]

Money mule recruitment

Research indicates that many victims of money mule recruitment come from financially vulnerable backgrounds, hence the increased appetite for quick or easy money; this includes fresh graduates, unemployed individuals, part-time workers, students, or debt-laden individuals.[604] Offenders are increasingly targeting young people (age group 21-30), but there are also reports of minors being recruited for money muling.[605] The Banking & Payments Federation Ireland estimates that almost a third of 18- 24-year-olds in Ireland have been approached for money muling or know someone who was.[606] In Belgium, 3% of respondents reported such approaches in 2023, rising to 4% in 2024, with consistently higher rates among young people.[607]

DM to collab bots

The primary targets of this scam are small content creators and micro-influencers with relatively low follower counts, who are particularly affected by their desire to grow their platforms. However, in practice, research finds that any social media user is exposed to bot-driven variations of this scheme.[608]

Unexpected gain scams

The primary targets of this scam category are individuals who may be more susceptible to promises of financial reward or windfall gains. According to a survey conducted by the Global Anti-Scam Alliance in 2025, unexpected money scams were experienced by 33%

[602] Euronews, Behind the global scam worth an estimated €100m targeting WhatsApp users with fake job offers (2023), available at: https://www.euronews.com/next/2023/10/23/behind-the-global-scam-worth-an-estimated-100m-targeting-whatsapp-users-with-fake-job-offe.

[603] JobScamScore, Job Scam Statistics 2026 (2026), available at: https://jobscamscore.com/guides/job-scam-statistics

[604] Eric Rutger Leukfeldt, Cybercrime and social ties. Phishing in Amsterdam (2014), available at: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/trndorgc17&section=22; Europol, Money Muling (2025), available at: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling.

[605] Europol, Money Muling (2025), available at: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling); The Guardian, 'Money mule' cases surge as criminals target young people on social media (2025), available at: https://www.theguardian.com/money/2025/dec/22/money-mule-cases-surge-as-criminals-target-young-people-on-social-media; VRT, Youngsters don't realise the risk of becoming a money mule (2022), available at: https://www.vrt.be/vrtnws/en/2022/11/29/_youngsters-don_t-realise-the-risk-of-becoming-a-money-mule/.

[606] Banking & Payments Federation Ireland, Almost €9.4m laundered through money mule accounts (2025), available at: https://bpfi.ie/money-mules-2025/.

[607] VRT, Youngsters don't realise the risk of becoming a money mule (2022), available at: https://www.vrt.be/vrtnws/en/2022/11/29/_youngsters-don_t-realise-the-risk-of-becoming-a-money-mule/.

[608] Bitdefender, How to Spot and Avoid Sponsorship Scams (2024), available at: https://www.bitdefender.co.uk/consumer/support/answer/107805/.

of respondents in the Netherlands, 35% in Italy, 38% in Spain, 40% in Germany, 42% in Denmark, 43% in Belgium, and 49% in France.[609]

Gambling scams

The primary targets of this type of scam are individuals engaged with online gambling or gaming-related content, as well as young people. Younger people, particularly those aged 16-24, are more likely to engage with gambling-like online environments and experience problem gambling behaviours, making them a higher-risk group for gambling-related harms.[610]

Charity and disaster relief scams

Fraudsters of charity and disaster relief scams exploit the generous behaviour of donors towards those in need. The affected users are not only the donors who incur financial loss, but also legitimate charities that are not receiving the actual donations.[611] Survey results from the 2025 reports of the GASA find that in the last twelve months, 41% of respondents in France, 38% in Italy and Belgium, 36% in Spain, 35% in Denmark and Germany, and 28% in the Netherlands have experienced a charity scam at least once.[612]

---

[609] GASA, State of Scams in the Netherlands (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_e4b2335bcebd496cab156f9a2440b6e1.pdf; GASA, State of Scams in Italy (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_90a4ada9f8be41b3b601995d679f5d30.pdf; GASA, State of Scams in Spain (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_737deba33aa546088296efc5ab7dff26.pdf; GASA, State of Scams in Germany (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_dbef245762ef487797354a803b67eb14.pdf; GASA, State of Scams in Denmark (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_3333c506a2274110988e0092bb9b04d4.pdf; GASA, State of Scams in Belgium (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_f4d15a699656439fb4ebfb9a5bdd55a1.pdf; GASA, State of Scams in France (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_fa620227910a4e8ebc06c0cd5e036614.pdf

[610] Heather Wardle & David Zendle, Loot Boxes, Gambling, and Problem Gambling Among Young People: Results from a Cross-Sectional Online Survey (2021), available at: https://journals.sagepub.com/doi/pdf/10.1089/cyber.2020.0299

[611] Europol, Online fraud schemes – A web of deceit (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/e914d7fe-b429-11ee-b164-01aa75ed71a1/language-en.

[612] GASA, State of Scams in the Netherlands (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_e4b2335bcebd496cab156f9a2440b6e1.pdf; GASA, State of Scams in Italy (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_90a4ada9f8be41b3b601995d679f5d30.pdf; GASA, State of Scams in Spain (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_737deba33aa546088296efc5ab7dff26.pdf; GASA, State of Scams in Germany (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_dbef245762ef487797354a803b67eb14.pdf; GASA, State of Scams in Denmark (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_3333c506a2274110988e0092bb9b04d4.pdf; GASA, State of Scams in Belgium (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_f4d15a699656439fb4ebfb9a5bdd55a1.pdf; GASA, State of Scams in France (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_fa620227910a4e8ebc06c0cd5e036614.pdf.

4.2. Economic impact of financial scams

Overall, estimates of the economic impact of financial scams should be interpreted with caution. **Due to significant levels of under-reporting, available figures remain indicative rather than precise, and the true scale of financial losses is likely to be substantially higher than recorded**. The following sections first examine the broader economic impact of online financial scams at the societal level, before moving to the individual-level economic impacts. The section concludes with available data on the economic impact associated with specific types of scams.

4.2.1. Societal-level economic impact

At the societal level, financial scams result in losses amounting to millions of euros each year.[613] At the international level, financial scams are estimated to generate losses of up to USD 1 trillion (EUR 0.9 trillion) annually, reflecting the growing role of organised crime and the rapid expansion of scams as a form of criminal activity.[614] In Europe, scams linked to impersonation are estimated to range between EUR 1 billion and EUR 27 billion in losses for EU citizens, while bank card payment scams account for between EUR 882 million and EUR 2 billion in losses. A joint EBA-ECB publication reported that the total value of payment scams increased to EUR 4.2 billion in 2025 from EUR 3.5 billion in 2023.[615] Further, after the takedown in 2022 by Europol of iSpoof.cc, a website that provided criminals with various services, including automated interactive voice response and live call monitoring, helping scammers to target victims worldwide, the site was estimated to have caused losses in excess of EUR 115 million.[616]

At the country-level, economic impact is also significant. In France, it was estimated that total losses suffered by victims of financial scams amount to at least EUR 500 million each year.[617] In Belgium, between July and December 2025, the Belgian financial authority reported that consumers lost more than EUR 23 million due to scams.[618] Identity theft alone is estimated to generate up to EUR 16 billion in indirect losses to EU citizens, largely due to lost income and time spent resolving cases. These impacts are

[613] Interview 7.

[614] Interview 4; see also GASA, Global State of Scams (2025), available at: https://gasa.org/knowledge-base/reports/global-state-of-scams-2025.

[615] ECB, Joint EBA-ECB report on payment fraud: strong authentication remains effective but fraudsters are adapting (2025), available at: https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr251215~e133d9d683.en.html.

[616] Europol, Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests (2022), available at: https://www.europol.europa.eu/media-press/newsroom/news/action-against-criminal-website-offered-%E2%80%98spoofing%E2%80%99-services-to-fraudsters-142-arrests

[617] Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes, Arnaques financières : les autorités mobilisées dans la lutte contre ce phénomène massif qui piège de plus en plus de particuliers (2024), available at: https://www.economie.gouv.fr/files/files/directions_services/dgccrf/media-document/cp-dgccrf-conference-afm.pdf.

[618] FSMA, Investment fraud and unlawful offers – Dashboard 2nd half of 2025 (2026), available at: https://www.fsma.be/sites/default/files/media/files/2026-01/20260122_dashboard_investment_fraud_2025_s2.pdf.

concentrated in France (24.8%), Germany (21.7%), Italy (9.6%), the Netherlands (9.1%), and Sweden (6%).[619] This concentration is likely driven by structural factors, such as their larger population sizes and higher volumes of online and financial activity, as well as potentially more developed reporting systems that capture scam incidents more comprehensively. In Germany, cybercrime-related scams induced financial loss of EUR 267 billion in 2024, 70% of which originated online.[620] In Ireland, estimated annual losses from payment scams range between EUR 100 million and EUR 150 million, although this is likely an underestimate due to under-reporting.[621] In Spain, online scams generate over EUR 350 million in economic losses each year, with some estimates placing total losses closer to EUR 500 million annually.[622] In Belgium, in 2023, EUR 40 million was still lost because of phishing, increasing to EUR 49 million in 2024.[623] Figures from Denmark indicate that DKK 464 million (EUR 62.1 million) was lost in 2023 due to online scams, a 30% increase from the year before.[624]

4.2.2. Individual-level economic impact

Across the European Union, the scale of direct financial harm is considerable. A rough estimation by the European Commission suggests that around 24% of individuals who experienced scams report some degree of financial loss. Most losses tend to be relatively small, with 11% losing less than EUR 50 and 10% losing between EUR 50 and EUR 500, while larger losses above EUR 500 are less common (3%).[625] Other findings indicate that 16% of victims suffer financial losses, with an average loss of EUR 650.[626] An EBA-

[619] European Commission, Study on online identity theft and identity related crime – Final report (2022), available at: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1/language-en

[620] BioCatch, Germans lose €267 billion to cybercrime (2025), available at: https://www.biocatch.com/press-release/germans-lose-267-billion-to-cybercrime

[621] Interview 4.

[622] Levanta la cabeza, El fraude digital aumenta un 40% en España: 1.200 estafas al día en 2025 (2025), available at: https://www.atresmedia.com/levanta-la-cabeza/buenas-practicas/ciberseguridad/fraude-digital-aumenta-40-espana-1200-estafas-dia-2025_202512306953a7ee22f0db7daf011949.html.

[623] Febelfin, Phishing & austres arnaques en vue (2024), available at: https://febelfin.be/media/pages/publicaties/2024/phishing-en-andere-kapers-op-de-kust/48633be3fd-1718872012/storytelling_phishing_fr_final.pdf.

[624] Finans Danmark, Styrket bekæmpelse af digital svindel - Svindel Task Forcens 18 anbefalinger (2024), available at: https://www.ft.dk/samling/20241/almdel/ERU/bilag/81/2948819/index.htm

[625] European Commission, Survey on 'Scams and Fraud Experienced by Consumers (2020), available at: https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf.

[626] Euroconsumers, Caught in the web: Navigating the digital maze of scams (2024), available at: https://www.euroconsumers.org/wp-content/uploads/2024/12/Caught-in-the-web-Navigating-the-digital-maze-of-scams.pdf

ECB joint report indicates that 85% of consumers ultimately bear the financial losses from payment fraud, with average losses exceeding EUR 1,000.[627]

Survey data at the national level indicate variations in both the share of victims incurring losses and the amounts lost. In France, Germany, and Belgium, 19% of adults report having lost money to scams in the past 12 months, with average losses of EUR 754.9, EUR 820, and EUR 2,041, respectively. In Sweden, 12% report losses, with an average of SEK 1545.4 (EUR 142), while in the Netherlands, 22% report losses, averaging EUR 802.[628] Based on the available data, no clear explanation can be established for why Belgium's average loss is more than double that of the other countries, as there are no significant differences in the prevalence of specific scam types that would account for this variation. In Spain, 51% of victims report losses exceeding EUR 147 per person, and the number of individuals involved as digital money mules increased sharply by nearly 1,000% between 2022 and 2024.[629] In Denmark, victims of online scams suffered an average loss of approximately DKK 8,180 (EUR 1,095) in 2025.[630]

In addition to immediate financial losses, scams can have longer-term economic consequences. Victims may lose savings, accumulate debt, and experience broader financial effects that extend to dependents and family members.[631]

For businesses and financial entities, scams generate both direct and indirect economic impacts. According to the European Union Agency for Cybersecurity, between January 2023 and June 2024, direct financial losses accounted for 13% of the economic impact, while large-scale financial losses represented 8%.[632] Direct losses arise from the theft of funds, ransom payments, and the costs associated with incident response and system recovery. In addition, financial organisations incur indirect costs, including increased

[627] ECB, Join EBA-ECB report on payment fraud: strong authentication remains effective but fraudsters are adapting (2025), available at: https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr251215~e133d9d683.en.html

[628] GASA, State of Scams in the Netherlands (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_e4b2335bcebd496cab156f9a2440b6e1.pdf; GASA, State of Scams in Italy (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_90a4ada9f8be41b3b601995d679f5d30.pdf; GASA, State of Scams in Spain (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_737deba33aa546088296efc5ab7dff26.pdf; GASA, State of Scams in Germany (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_dbef245762ef487797354a803b67eb14.pdf; GASA, State of Scams in Denmark (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_3333c506a2274110988e0092bb9b04d4.pdf; GASA, State of Scams in Belgium (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_f4d15a699656439fb4ebfb9a5bdd55a1.pdf; GASA, State of Scams in France (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_fa620227910a4e8ebc06c0cd5e036614.pdf

[629] Levanta la cabeza, El fraude digital aumenta un 40% en España: 1.200 estafas al día en 2025 (2025), available at: https://www.atresmedia.com/levanta-la-cabeza/buenas-practicas/ciberseguridad/fraude-digital-aumenta-40-espana-1200-estafas-dia-2025_202512306953a7ee22f0db7daf011949.html.

[630] This figure is calculated based on self-reported loss amounts in the survey available at: https://taenk.dk/system/files?file=2025-05/Digital%20svindel%20i%20Danmark_FINAL_290425.pdf

[631] Oak & Shafiq,"Hello, is this Anna?: Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf

[632] ENISA, Threat Landscape 2024 (2024), available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

insurance premiums, regulatory fines, and long-term reputational damage.[633] Overall, according to estimates from the European Commission, losses arising from identity fraud are likely to amount to more than EUR 10,000 per affected business/corporation in certain Member States.[634] One identity fraud attempt can generate costs ranging between EUR 1,200 and EUR 6,000 for each affected EU-based business.[635] The cost of credential theft is about EUR 400,000 per company.[636] Isolated cases can depict the reach of scams on businesses. In France, in 2021, scammers using deepfake audio to impersonate the CEO of a company elicited the transfer of around EUR 35 million.[637] In Finland, in 2020, scammers exploited a data breach of a mental health service provider and extorted patients to pay a total of EUR 450,000 in bitcoin.[638]

4.2.3. Economic impact by type of scam

The scale of the **economic harm experienced by victims may vary depending on the type of scam.** The following sections examine the individual and societal impacts associated with different scam types. Please note that data is not available for all scam types included in the typology. Therefore, only those for which data is available are discussed below.

Investment scams

Traditional investment scams

Overall, in 2024, online investment scam losses were estimated at EUR 4 billion in Europe.[639] In March 2023, a coordinated action by Europol and Eurojust took down a fraudulent online investment platform that had targeted at least 33,000 victims for an estimated loss of EUR 89 million in illicit profits.[640] Reported damages from investment scams in Austria reached EUR 120 million in 2024, although this reflects only reported

[633] ibid.

[634] European Commission, Study on online identity theft and identity related crime – Final report (2022), available at: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1/language-en.

[635] ibid.

[636] ibid.

[637] Europol, Franco-Israeli gang behind EUR 38 million CEO fraud busted (2023), available at: https://www.europol.europa.eu/media-press/newsroom/news/franco-israeli-gang-behind-eur-38-million-ceo-fraud-busted

[638] European Commission, Study on online identity theft and identity related crime – Final report (2022), available at: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1/language-en

[639] Investigate Europe, Scam Europe (2025), available at: https://www.investigate-europe.eu/themes/investigations/-scam-europe

[640] Europol, Further action against fraudulent online investment platform: five arrest of high-value targets (2023), available at: https://www.europol.europa.eu/media-press/newsroom/news/further-action-against-fraudulent-online-investment-platform-five-arrests-of-high-value-targets

cases and likely underestimates the true scale.[641] Data from the Danish financial authority shows that in 2020, DKK 67.9 million (EUR 9 million) was lost due to investment scams, DKK 59.4 million in 2021 (EUR 7.9 million), DKK 44.7 million in 2022 (EUR 6 million), DKK 47.7 million in 2023 (EUR 6.4 million), DKK 95 million in 2024 (EUR 12.7 million) and DKK 36.4 million in 2025 (EUR 4.9 million), indicating the absence of a steady trend across the years.[642] In Sweden, in 2025, profits generated from investment scams were estimated at SEK 1.6 billion (EUR 147 million), which is 6% more than in 2024.[643] Finally, in the Netherlands, the Dutch Authority for the Financial Markets estimates that investment scams caused losses of EUR 750 million per year.[644]

Cryptocurrency scams

Cryptocurrency-related scams represent a rapidly growing category of financial loss in recent years.[645] The scale, reach, and technical characteristics of cryptocurrency scams present great challenges for law enforcement and financial systems, particularly because the use of anonymous, hard-to-trace channels makes it difficult to track illicit funds, thereby facilitating money laundering and limiting asset recovery. Cryptocurrency anonymity also creates a new money laundering problem for banking, law enforcement, and the legal system.[646] Globally, Chainalysis estimates that USD 17 billion (EUR 15 billion) was stolen through cryptocurrency scams in 2025 alone.[647] Overall, estimated financial losses from cryptocurrency scams increased from around USD 12 billion (EUR 10 billion) in 2024 to USD 17 billion (EUR 15 billion) in 2025 worldwide.[648] In 2025, Eurojust, together with French, Belgian, Cypriot, German and Spanish authorities, dismantled a cryptocurrency money laundering network that scammed victims of over

[641] Interview 5.

[642] Finans Danmark, Styrket bekæmpelse af digital svindel - Svindel Task Forcens 18 anbefalinger (2024), available at: https://www.ft.dk/samling/20241/almdel/ERU/bilag/81/2948819/index.htm

[643] Polisen, Bedrägeribrottslighetens vinster sjunker för andra året i rad (2026), available at: https://polisen.se/aktuellt/nyheter/nationell/2026/april/bedrageribrottslighetens-vinster-sjunker-for-andra-aret-i-rad/

[644] AFM, Investment fraud: losses likely in the hundreds of millions of euros per year (2025), available at: https://www.afm.nl/en/sector/actueel/2025/dec/pb-beleggingsfraude

[645] Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en.

[646] Vasilka Chergarova et al., Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest in cryptocurrency (2022), available at: https://iacis.org/iis/2022/3_iis_2022_242-252.pdf.

[647] Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/.

[648] Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/.

EUR 600 million.[649] Data from the financial authority in Belgium reports that in 2025, more than EUR 10.5 million was lost in investments linked to cryptocurrency.[650]

Romance scams

Traditional romance scams

According to the GASA survey, in 2025, reported romance scam victimisation rates reached 27% in Spain, 28% in the Netherlands, 30% in Denmark, 34% in France, 36% in Belgium, and 37% in Germany.[651] Financial losses are substantial, with reported losses exceeding EUR 13.6 million in Finland in 2025[652], SEK 551 million (EUR 50 million) in Sweden in 2025[653], USD 600 million (EUR 556 million) in the United States, GBP 68 million (EUR 82 million) in the United Kingdom, and AUD 131 million (EUR 77 million) in Australia in 2021, although under-reporting suggests that actual figures are considerably higher.[654] Further upward trends were observed in the United Kingdom, with reports of romance scams increasing by 73% during 2021, compared with 2020, totalling GBP 30.9 million (EUR 37 million) lost and case numbers jumping to 41%.[655] In Denmark, romance scam losses rose from DKK 6.6 million (EUR 883,514) in 2020 to

[649] Eurojust, Decisive actions against cryptocurrency scammers earning over EUR 600 million (2025), available at: https://www.eurojust.europa.eu/news/decisive-actions-against-cryptocurrency-scammers-earning-over-eur-600-million

[650] FSMA, Investment fraud and unlawful offers – Dashboard 2nd half of 2025 (2026), available at: https://www.fsma.be/sites/default/files/media/files/2026-01/20260122_dashboard_investment_fraud_2025_s2.pdf.

[651] Global Anti-Scam Alliance, State of Scams in The Netherlands – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_e4b2335bcebd496cab156f9a2440b6e1.pdf; Global Anti-Scam Alliance, State of Scams in Germany – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_dbef245762ef487797354a803b67eb14.pdf; Global Anti-Scam Alliance, State of Scams in Spain – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_737deba33aa546088296efc5ab7dff26.pdf; Global Anti-Scam Alliance, State of Scams in France – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_fa620227910a4e8ebc06c0cd5e036614.pdf; Global Anti-Scam Alliance, State of Scams in Italy – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_90a4ada9f8be41b3b601995d679f5d30.pdf; Global Anti-Scam Alliance, State of Scams in Belgium – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_f4d15a699656439fb4ebfb9a5bdd55a1.pdf.

[652] Poliisi, Information and open discussion are key factors in combatting online scams (2026), available at: https://poliisi.fi/en/-/information-and-open-discussion-are-key-factors-in-combatting-online-scams

[653] Polisen, Brottsvinsterna för bedrägeribrottsligheten 2025 (2026), available at: https://polisen.se/e138feea53c6c74289ea158bf6059519/siteassets/dokument/ovriga_rapporter/brottsvinsterna-for-bedrageribrottsligheten-2025.pdf

[654] Cassandra Cross and Karen Holt, To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581.

[655] Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670.

DKK 7.1 million (EUR 950125) in 2025, indicating a steady increase across the years.[656] In Sweden, in 2025, profits generated from romance scams were estimated at SEK 551 million (EUR 50 million), which represents 48% more than in 2024.[657] In the Netherlands in 2023, 494 cases of romance scams were recorded, with 264 victims suffering financial losses totalling EUR 7,644,870. This corresponds to an average loss of nearly EUR 29,000 per victim, which can lead to long-term financial difficulties.[658] In exceptional cases, individual losses have been reported to reach as high as EUR 120,000 in Belgium.[659]

E-commerce scams

Undelivered products or services

Data from the Dutch Fraud Help Desk indicates that the average financial harm caused by non-delivery scams reached approximately EUR 350 per victim in 2023.[660] However, the aggregated financial loss ranks highly, particularly considering the high volume of scams. For example, the BogusBazaar operation, a China-based "infrastructure-as-a-service" fraud network, operated over 75,000 fake online shops impersonating well-known brands to harvest payment card details and collect payment for goods that were never delivered.[661] This operation alone processed over USD 50 million (EUR 43 million) in fake orders between 2021 and 2024 (see case study C in Section 6.3 for further analysis).[662]

Counterfeit product scams

The impact of counterfeit product scams is wide-ranging. In terms of financial damage, the EU reported seizing over 112 million counterfeit articles in 2024 alone, with an estimated retail value of EUR 3.8 billion.[663] Victims suffer direct financial losses, and on

[656] Finans Danmark, Styrket bekæmpelse af digital svindel - Svindel Task Forcens 18 anbefalinger (2024), available at: https://www.ft.dk/samling/20241/almdel/ERU/bilag/81/2948819/index.htm

[657] Polisen, Bedrägeribrottslighetens vinster sjunker för andra året i rad (2026), available at: https://polisen.se/aktuellt/nyheter/nationell/2026/april/bedrageribrottslighetens-vinster-sjunker-for-andra-aret-i-rad/

[658] Fraudehelpdesk, In 2023 bedroeg schade datingfraude méér dan 7 miljoen euro, 75% meer dan in 2022 (2024), available at: https://www.fraudehelpdesk.nl/wp-content/uploads/2024/02/Persbericht-campagne-datingfraude-5-2-24.pdf

[659] Schokkenbroek & Snaphaan, Love as Bait: A Scoping Review and Crime Script Analysis of Online Romance Scams (2025), available at: https://journals.sagepub.com/doi/full/10.1177/15248380251361046

[660] Autoriteit Consument en Markt, Consumer organizations warn against untrustworthy online stores (2023), available at: https://www.acm.nl/en/publications/consumer-organizations-warn-against-untrustworthy-online-stores.

[661] Business Insider, A Chinese criminal ring has stolen $50 million by franchising thousands of fake online shops, experts say (2024), available at: https://www.businessinsider.com/fake-online-shops-china-crime-ring-franchise-model-target-americans-2024-5.

[662] ibid.

[663] European Union Intellectual Property Office, EU Enforcement of Intellectual Property Rights – Results at the EU Border and in the EU Internal Market 2024 (2025), available at: https://euipo.europa.eu/tunnel-

top of this, they typically do not receive the goods they thought they paid for. In fact, because the offenders are usually based outside the EU, any goods that are shipped risk being intercepted at customs and destroyed.[664]

Health and wellness scams

In relation to health and wellness scams, the financial impact of fake medicines offered online ranks highly. In 2024, the coordinated efforts under Operation SHIELD V (led by Europol) single-handedly led to the seizure of fake medicinal products worth above EUR 11.1 million.[665]

Event ticket scams

In addition, event ticket scams have become a significant problem across Europe, generating important financial losses and hampering consumer trust. While no EU-wide estimate of losses specific to ticket scams is available, data at the national level illustrates the scale of the phenomenon. For example, Action Fraud (UK national fraud and cybercrime reporting service) published data indicating that event ticket scam losses amounted to GBP 9.7 million (EUR 11 million) in 2024, of which GBP 1.6 million (EUR 1.8 million) related to concerts.[666] In Belgium, the financial damage reported by victims reached more than EUR 60,000 in 2023, almost five times more than in 2022.[667] However, the financial loss incurred by victims may not be limited to the value of the fake tickets they have acquired, especially if they have made travel or accommodation plans for the event they wanted to attend. As such, while the Belgian authorities estimated in 2023 the average loss resulting from ticket scams at EUR 168 per person, that number may be higher in practice.[668]

Insurance scams

Online insurance scams often cause high financial losses, which go beyond the price of the false insurance policy; however, estimates as to these losses have not yet been quantified. Often, victims do not realise they have been scammed until they try to make

web/secure/webdav/guest/document_library/observatory/documents/reports/2025_EU_Enforcement_report/EU_enforcement_of_IPRs:_results_at_EU_border_&_EU_internal_market_2024_en.pdf.

[664] ibid.

[665] Europol, Europol warns consumers to be mindful about fake medicines offered online (2025), available at: https://www.europol.europa.eu/media-press/newsroom/news/europol-warns-consumers-to-be-mindful-about-fake-medicines-offered-online.

[666] UK Government, £1.6m lost to gig ticket scams as public urged to take caution (2025), available at: https://www.gov.uk/government/news/16m-lost-to-gig-ticket-scams-as-public-urged-to-take-caution; Bitdefender, Action Fraud Urges Vigilance as Ticket Fraud Losses Surge to £9.7 Million (2025), available at: https://www.bitdefender.com/en-gb/blog/hotforsecurity/action-fraud-urges-vigilance-as-ticket-fraud-losses-surge-to-9-7-million.

[667] RTBF, Les signalements de fraude aux tickets de concerts ont doublé en un an : "J'ai perdu 180 euros et je n'ai jamais reçu mes places" (2024), available at : https://www.rtbf.be/article/les-signalements-de-fraude-aux-tickets-de-concerts-ont-double-en-un-an-j-ai-perdu-180-et-je-n-ai-jamais-recu-mes-places-11394129.

[668] ibid.

a claim in the event of an accident; then, they have to pay out of pocket for their losses and for a new, valid insurance policy.[669]

Loan and credit offer scams

With regard to loan and credit offer scams, beyond the loss of the upfront fee, victims are left without the funds they urgently needed. In France, data from the first three quarters of 2024 indicates an average financial loss of EUR 19,000 per victim, depicting the significant monetary damage that this type of scam can inflict.[670]

Rental scams

No EU-level data on average financial losses per victim of fake listing rental scams is currently available. Evidence is limited to case-based law enforcement investigations and national reporting. For instance, Europol's investigations into cross-border holiday rental scams operated from Romania through fake listings that targeted victims from other Member States have documented individual losses ranging between EUR 200 and EUR 10,000 per victim, generating illicit profits estimated in the millions of euros.[671] Beyond direct financial loss, harm typically includes significant practical disruption when victims discover, upon arrival, that the listing was not real and that they are left without accommodation.

In relation to phishing campaigns carried out through accommodation platforms, Altroconsumo reports that some victims lost more than EUR 1,500.[672] Beyond the financial loss associated with the false payment, victims also face privacy and security harms, as their personal information, including credit card data, is harvested by scammers through the cloned interfaces.[673]

Employment and collaboration scams

Fake job scams

Fake job scams cause significant financial damage, directly in terms of the sums the victims pay for the false onboarding processes, but also indirectly through the use of their information for subsequent criminal purposes. For example, in the US, consumer losses

[669] Insurance Europe, Insurance Europe response to EC consultation on online fraud (2026), available at: https://www.insuranceeurope.eu/mediaitem/c356079f-c353-4754-a049-1a0054e0b29b/Insurance+Europe+response+to+EC+consultation+on+online+fraud.pdf?inline=1.

[670] L'Autorité de contrôle prudentiel et de résolution (ACPR), L'ACPR met en garde le public contre la multiplication de fausses offres de prêt immobilier ou de rachat de crédit proposées par des individus usurpant l'identité de courtiers et d'établissements de crédit (2024), available at: https://acpr.banque-france.fr/fr/communiques-de-presse/lacpr-met-en-garde-le-public-contre-la-multiplication-de-fausses-offres-de-pret-immobilier-ou-de.

[671] Europol, Busted: 9 arrested in hit against holiday-rental fraudsters (2024), available at: https://www.europol.europa.eu/media-press/newsroom/news/busted-9-arrested-in-hit-against-holiday-rental-fraudsters

[672] Altroconsumo, Prenotazioni su Booking.com: occhio alla truffa del sito clone (2025), available at: https://www.altroconsumo.it/soldi/truffe/news/truffa-sito-booking-clone.

[673] Euroconsumers, Form fraud is rife on booking.com: Your scam stories can help to stop criminals (2025), available at: https://www.euroconsumers.org/fraud-booking-com-share-scam-stories/.

to job scams are estimated at more than USD 264 million (EUR 227 million) in 2024.[674] Unfortunately, data at a European level is not yet available.

Charity and disaster relief scams

Charity scams

In the UK, the Charity Fraud Survey notes that 34% of charities reported fraud or attempted fraud in 2025, causing financial loss for 73% of them, with an average loss between GBP 11,000 and GBP 110,000 (EUR 12,670-126,720).[675] Unfortunately, data at a European level is not yet available.

Crowdfunding scams enable fraudsters to collect small sums from a large number of people. Some emblematic examples were found outside of Europe. For example, in the US, one fraudulent crowdfunding campaign ('Pay It Forward') on the platform GoFundMe raised more than USD 400,000 (EUR 370,000), following which the offenders were prosecuted, and the donors received a full refund. GoFundMe reported that such misuse was rare, accounting for less than 0.1% of all campaigns on the platform.[676] As another example, the ''Kobe red beef jerky'' campaign by Magnus Inc., which claimed to offer fresh Kobe beef-based jerky from Japan, almost achieved USD 120,309 (EUR 111,428) on the Kickstarter platform from 3,252 donors in less than a month. Fortunately, Kickstarter spotted this scam just one day before the fundraising completion, following a documentary film that investigated the legitimacy of the campaign.[677] Data on the losses associated with crowdfunding scams at the European level is not yet available.

4.3. Social impact of financial scams

Similar to the economic impact sections, the analysis of the social impact of financial victims should be read with caution. Since the scam landscape keeps evolving, the social impact of some types of scams may have been more studied than others. Moreover, the effects of victimisation have often been studied against non-random samples, so their characteristics are likely to be more severe. The following sections first examine the societal harms associated with financial scams, then focus on individual-level social impacts, and finally present available evidence on social impacts by type of scam.

[674] US Federal Bureau of Investigation, Internet Crime Report 2024, available at: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.

[675] BDO, Fraud Advisory Panel, Charity Fraud Report: a five-year review (2026), available at: https://www.bdo.co.uk/getmedia/622cc7e5-f5fc-4bf3-87bc-f92dfffb95e4/NFP-Report-BDO-Charity-Fraud-Report-2025.pdf

[676] CNBC, On #GivingTuesday, check into that crowdfunding campaign before you donate (2018), available at: https://www.cnbc.com/2018/11/27/how-to-avoid-fraud-on-crowdfunding-sites.html.

[677] Seunghun Lee et al., Fraud Detection on Crowdfunding Platforms Using Multiple Feature Selection Methods (2025), available at: https://xplorestaging.ieee.org/ielx8/6287639/10820123/10909102.pdf?arnumber=10909102&utm_source=scopus&getft_integrator=scopus

4.3.1. Societal-level social impacts

Scams not only cause direct harm to those exposed but also have an impact on buying behaviour and hence the functioning of the Internal Market. EU-level survey data reports that almost **four in ten people who experienced scams (38%) felt that this affected their online buying behaviour.** Even more striking is that more than half (53%) of those who experienced an online buying scam changed their online buying behaviour, underlining the substantial impact scams may have on consumers' trust in the market.[678] According to the EU FRA consumer survey, one in three victims (34%) of online scams reported changing their online behaviour after experiencing the scam.[679] One interviewee indicated that **victims of online financial scams become more cautious but might also withdraw from online interactions, leading to reduced engagement with digital and financial systems**.[680] This may contribute to broader changes in user behaviour and a broader erosion of trust in oneself and in others.[681] According to the EU FRA consumer survey, 28% of victims reported feeling a loss of trust because of experiencing online scams.[682] Another interviewee noted that trust in media and digital platforms may be further undermined by the use of impersonation techniques, where scammers replicate the identity of trusted organisations to increase credibility.[683] The aggregated effect of disengagement decisions may consequently lead to a decrease in trust in online platforms, financial institutions, and, more broadly, institutional systems.[684]

At a broader level, scams contribute to the financing of other criminal activities and reinforce a cycle of mistrust in the system. The cumulative effect is a **weakening of confidence in digital environments and a reluctance among individuals to engage fully in online economic and social activities**.[685]

4.3.2. Individual-level social impacts

At the individual level, the consequences of financial scams extend far beyond monetary loss. Victims frequently experience emotional distress, reputational damage, and, in some cases, safety risks, particularly where scams intersect with critical

[678] European Commission, Survey on "scams and fraud experienced by consumers" – Final Report (2020, available at: https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

[679] European Union Agency for Fundamental Rights, Online Fraud – People's experiences across the EU (2026), available at: https://fra.europa.eu/en/publication/2026/victims-online-fraud.

[680] Interview 2.

[681] Interview 4.

[682] European Union Agency for Fundamental Rights, Online Fraud – People's experiences across the EU (2026), available at: https://fra.europa.eu/en/publication/2026/victims-online-fraud.

[683] Interview 5.

[684] Interviews 7, 9; see also ECC-Net, The impact of counterfeiting on online consumer rights in Europe (2017), available at: https://www.eccbelgium.be/brochures/detail/ecc-net-report-the-impact-of-counterfeiting-on-online-consumer-rights-in-europe.

[685] Interview 7.

infrastructures.[686] Victims also report feelings of shame, stress, betrayal, anxiety, and depression.[687] Specifically, EU survey-level data reports that around 79% of individuals who experience scams report some form of emotional harm, most commonly irritation (68%), anger (56%), stress (30%), and embarrassment (16%).[688] Physical health effects are also reported, though less frequently, with 6% indicating impacts such as sleep disturbances, fatigue, or headaches.[689] Physical health effects can also emerge from consumers buying counterfeit goods, such as counterfeit cosmetics or health products, which may contain harmful substances, such as incorrect dosages or harmful chemicals, and can lead to life-threatening conditions.[690] Beyond emotional and physical detriment, victims also experience reputational harm, especially in cases involving impersonation or identity theft, which may lead to isolation, depression, or a diminished sense of self-worth. In severe cases, social impacts include post-traumatic stress, loss of confidence, and suicidal thoughts or actions.[691] Victims may also become more vulnerable to harmful or extremist ideologies where their trust in institutions has been undermined.[692]

The emotional impact of scams is often intensified by a lack of social support, not only from friends and family, but also from authorities and formal support channels. **Victims may feel ashamed or reluctant to share their experiences and may encounter misunderstanding or blame when they do.** This form of secondary victimisation, where responsibility is attributed to the victim or their judgement is questioned, deepens the impact and discourages reporting.[693] Feelings of shame and lack of trust further contribute to under-reporting. Victims may also be targeted again through recovery scams, in which fraudsters exploit prior victimisation by offering false opportunities to recover lost funds in exchange for upfront payments, such as fees, taxes, or administrative costs.[694] Re-victimisation not only increases the financial damage but also aggravates the psychological and emotional trauma experienced by the victims.[695] A further consequence is the development of learned helplessness, where individuals

[686] Interviews 1, 2.

[687] Interviews 5, 7.

[688] European Commission, Survey on 'Scams and Fraud Experienced by Consumers' (2020), available at: https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf.

[689] ibid.

[690] ECC-Net, The impact of counterfeiting on online consumer rights in Europe (2017), available at: https://www.eccbelgium.be/brochures/detail/ecc-net-report-the-impact-of-counterfeiting-on-online-consumer-rights-in-europe.

[691] Interviews 2, 4.

[692] Interview 2.

[693] Interview 1; see also Drew & Webster, The victimology of online fraud: A focus on romance fraud victimisation (2024), available at: https://www.sciencedirect.com/science/article/pii/S2949791424000058;

[694] Interview 1; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[695] Interpol, Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/content/download/21096/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03_EN_v3.pdf

perceive victimisation as unavoidable, reducing preventive behaviour and increasing anxiety in digital interactions.[696]

Beyond emotional and psychological harm, scams may also produce tangible **legal and administrative consequences**. Victims of impersonation or identity theft can face civil or criminal complications, including false accusations, damaged credit records, or legal disputes arising from fraudulent contracts or accounts created in their name. Resolving such issues often requires significant time and effort, adding to the overall psychological and financial burden.[697] When buying counterfeit goods, consumers might be involved in the infringement of intellectual property rights, which can result in legal actions against the consumer.[698]

For businesses and financial entities, financial scams also have far-reaching consequences by compromising operational efficiency, regulatory compliance, consumer trust, and reputational damage.[699] Between January 2023 and June 2024, the European Union Agency for Cybersecurity identified operational disruption as the most common impact, affecting 58% of cases.[700] This was followed by the exposure and sale of sensitive data (17%), reputational damage (13%), and regulatory and compliance penalties (1%).[701] It should be noted that these impacts are similar for both online and offline financial scams.[702]

4.3.3. Social impact by type of scam

While the general societal and individual-level impacts described above can be considered generally applicable to victims of any type of scam, the following sections provide additional information on the social impacts associated with a specific scam type. The scale and reach of certain scams mean that their impacts may be more pronounced compared to others. Therefore, the sections below outline individual and societal-level impacts by scam type. Only scam types for which additional data is available are included.

---

[696] European Commission, Survey on 'Scams and Fraud Experienced by Consumers' (2020), available at: https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf.

[697] ibid.

[698] ECC-Net, The impact of counterfeiting on online consumer rights in Europe (2017), available at: https://www.eccbelgium.be/brochures/detail/ecc-net-report-the-impact-of-counterfeiting-on-online-consumer-rights-in-europe.

[699] ENISA, Threat Landscape 2024 (2024), available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024; Amos Kipngetich, A review of online scams and financial frauds in the digital age (2025), available at: https://gsconlinepress.com/journals/gscarr/sites/default/files/GSCARR-2025-0025.pdf.

[700] ENISA, Threat Landscape 2024 (2024), available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[701] ibid.

[702] Levi Michael, Frauds and Their Controls: Some Scholarly Reflections (2025), available at: https://www.journals.uchicago.edu/doi/10.1086/736347

Investment scams

Traditional investment scams

Investment scams share the psychological and social consequences described above, including depression, anxiety, trauma, isolation, damaged relationships, and behavioural changes.[703] Victims are also disproportionately targeted for re-victimisation through recovery scams, as described in Section 4.3.2 above.[704]

Romance scams

Traditional romance scams

Romance scams involve a level of emotional and sexual connection that is not typically present in other types of scams and implies a greater direct impact on victims.[705] Victims of romance scams are often cited as facing particularly serious psychological and emotional consequences, as the scam involves the development of a romantic relationship with the offender. The emotional impact is compounded by the perceived betrayal and loss of a genuine romantic connection, which many victims identify as the most difficult aspect of the experience, often exceeding the burden of financial loss.[706] In some cases, victims may also find it challenging to distinguish between the fabricated identity and the individual responsible for the deception.[707] Notably, even victims who did not suffer financial loss report significant emotional distress. Romance scams are therefore often described as involving a 'double hit' of victimisation, whereby victims must not only grieve the loss of any money, but they also grieve the loss of the relationship.[708] Furthermore, victims can experience acute and ongoing fear of their physical safety and

[703] Luke Balcombe, The mental health impacts of internet scams (2025), available at: https://www.mdpi.com/1660-4601/22/6/938; Antonis Papasavva et al., Applications of AI-Based Models for Online Fraud Detection and Analysis (2025), available at: https://link.springer.com/content/pdf/10.1186/s40163-025-00248-8.pdf.

[704] Watchlist Internet, Die Evolution des Online-Betrugs: Vom klassischen Internetbetrug zur KI-gestützten Täuschung (2024), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Bericht_KI_und_Betrug_final.pdf.

[705] Lazarus et al. What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021) (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000131.

[706] Monica Whitty, The online dating romance scam: The psychological impact on victims–both financial and non-financial (2015), available at: https://journals.sagepub.com/doi/abs/10.1177/1748895815603773.

[707] Rasha Kassem and Elisabeth Carter, Mapping romance fraud research – a systematic review (2024), available at: https://www.emerald.com/jfc/article-abstract/31/4/974/1238258/Mapping-romance-fraud-research-a-systematic-review?redirectedFrom=fulltext.

[708] Drew & Webster, The victimology of online fraud: A focus on romance fraud victimisation (2024), available at: https://www.sciencedirect.com/science/article/pii/S2949791424000058; Monica Whitty, A systematic literature review of profiling victims of cyber scams: setting up a framework for future research (2025), available at: https://www.tandfonline.com/doi/pdf/10.1080/23311886.2025.2563781; Schokkenbroek & Snaphaan, Love as Bait: A Scoping Review and Crime Script Analysis of Online Romance Scams (2025), available at: https://journals.sagepub.com/doi/full/10.1177/15248380251361046; Cassandra Cross and Karen Holt, To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581.

may be involuntarily involved in money laundering and the delivery of illegal goods, hence becoming unknowingly complicit in serious crimes.[709]

Romance baiting

The impact of romance baiting is particularly severe due to the combination of emotional and financial harm. The dual nature of these scams amplifies their overall impact, as victims experience both financial exploitation and the breakdown of a perceived personal relationship. Victims are often targeted over extended periods, leading to substantial financial losses and long-term mental health issues.[710]

E-commerce scams

Undelivered products or services

Victims of undelivered product scams may face secondary harm from the subsequent exploitation of stolen payment data for further fraudulent transactions. The difficulty of obtaining recourse once a payment has been made to a fraudulent site is a consistent feature of victim experiences, and a structural challenge for enforcement.[711]

Counterfeit products or services

The proliferation of counterfeit goods can devalue authentic products, thereby causing reputational damage to legitimate e-commerce platforms.[712] A tangible health and safety dimension must also be considered: counterfeit products often do not comply with EU safety regulations, meaning that elements such as helmets or electronics may pose direct physical risk to consumers.[713]

Health and wellness scams

Victims of health and wellness scams may suffer significant psychological harm, as they may experience anxiety over the effects of taking substandard medications.[714] At the aggregated level, such scams constitute a public health threat, as they may increase the general burden of illness within society.[715] At the same time, the growing reliance on self-medication among the general population has contributed to the proliferation of falsified

[709] Rasha Kassem and Elisabeth Carter, Mapping romance fraud research – a systematic review (2024), available at: https://www.emerald.com/jfc/article-abstract/31/4/974/1238258/Mapping-romance-fraud-research-a-systematic-review?redirectedFrom=fulltext.

[710] Bhupendra Acharya and Thorsten Holz, An Explorative Study of Pig Butchering Scams (2024), available at: https://arxiv.org/pdf/2412.15423.

[711] ECC-Net, Fraud in Cross-border E-commerce (2016), available at: https://www.eccnet.eu/publication/online-fraud; Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[712] Ani Khachatryan, The Digital Dilemma: Counterfeit Culture and Brand Protection Reform in the E-Commerce Era (2023), available at: https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1659&context=elr.

[713] ibid.

[714] Ankit Raj et al., Counterfeit medicine: a major public health concern and effective remedies for combatting the crisis (2025), available at: https://link.springer.com/article/10.1007/s44395-025-00004-6.

[715] ibid.

or counterfeit medical and wellness products, which are often manufactured in unregulated underground laboratories without appropriate safety standards. As a result, consumers may be exposed to serious risks, including treatment failure, toxicity, or death, posing substantial threats to public health.[716]

Artificial streaming scams

Artificial streaming scams negatively impact other content creators, whose ability to reach broader audiences and to benefit from platforms' monetisation systems may be hindered.[717] As recommender algorithms and monetisation systems reward and prioritise engagement and popularity, content creators that solely rely on authentic engagement may find themselves at a disadvantage when competing with creators that rely on bots to falsely inflate their engagement rates. This disadvantage may translate into missing out on lucrative advertisement opportunities and in the downranking of their posts. The harmful impact of inauthentic engagement has been legally recognised, with the US Federal Trade Commission explicitly declaring this practice unlawful.[718]

Insurance scams

Insurance scams can have dire consequences. In the case of fraudulent car insurance policies, driving without valid insurance may constitute a criminal offence and can result in significant penalties, including fines, vehicle seizure, driving bans, or imprisonment.[719] In addition, parties involved in road traffic accidents may face difficulties in obtaining compensation for personal injury or vehicle repair claims where insurance coverage is invalid or non-existent.

Employment and collaboration scams

Fake job scams

Fake job scams can lead to significant distrust in the job market. Victims of fake job scams report that the ubiquity of fraudulent job listings discourages them from continuing to look for a job, and that they experience an increased need for hypervigilance when interacting with potential employers.[720]

---

[716] Aonghus J Feeney et al., Global perspective of the risks of falsified and counterfeit medicines: A critical review of the literature (2024), available at: https://www.sciencedirect.com/science/article/pii/S1477893924000759.

[717] StreamCharts, The Hidden Cost of Viewbotting (2025), available at: https://streamscharts.com/reports/viewbotting-whitepaper.

[718] US Federal Trade Commission, Trade Regulation Rule on the Use of Consumer Reviews and Testimonials 16 CFR Part 465, 22 August 2024, available at: https://www.federalregister.gov/documents/2024/08/22/2024-18519/trade-regulation-rule-on-the-use-of-consumer-reviews-and-testimonials.

[719] ibid; Insurance Fraud Bureau, Don't be caught out by fake car insurance - The Result Could Be Crushing, available at: https://www.insurancefraudbureau.org/en/ghost-broking.

[720] Alexandrea J Ravanelle et al., Good jobs, scam jobs: Detecting, normalizing, and internalizing online job scams during the COVID-19 pandemic (2022), available at: https://journals.sagepub.com/doi/pdf/10.1177/14614448221099223.

5. Countermeasures

Articles 34 and 35 DSA require VLOPs and VLOSEs to identify systemic risks and implement reasonable, proportionate, and effective mitigation measures. These obligations are technology-neutral and may be fulfilled through a combination of regulatory compliance measures and platform-specific (voluntary or design-driven) enforcement tools. In practice, platforms deploy a hybrid approach in which regulatory obligations are operationalised through proprietary detection systems, internal policies, and voluntary industry practices.

As a disclaimer, the study does not assess or evaluate the compliance of any online platforms or online search engines with the obligations they incur under the DSA. The following section aims to provide a neutral overview of the current landscape of available countermeasures.

To that end, the following sections distinguish between four categories of countermeasures relevant to the online financial scam phenomenon, with delineations drawn between categories by reference to their function and point of contact with scam content. For each category of countermeasures, the report identifies different types of measures, separately providing overviews of the data on their implementation, as published by the designated services, and as observed by relevant stakeholders. For each type of countermeasures, a table overview of its implementation by designated services is provided in Annex V. Each table compiles information from the reports and policies made publicly available by designated service providers.

5.1. Access and gatekeeping measures

Access and gatekeeping measures represent the first line of defence against online financial scams by controlling who and what can reach users on a platform. Rather than targeting scam content after it has been published, **these measures operate upstream, imposing conditions that must be met before individuals and/or businesses can create accounts or post content on the designated services**. This category of countermeasures includes identity requirements for personal accounts, Know Your Business Customer (KYBC) processes, ad placement requirements and AI labelling measures. Together, these measures function as a series of gates that scam operators must pass through or circumvent, with each layer envisioned to reduce the volume and credibility of fraudulent content that ultimately reaches end users.

Measure 1: Identity requirements for personal accounts

General overview

High-assurance identity verification upon account creation refers to **measures requiring or allowing users (depending on the configuration of the measure) to confirm their identity using reliable credentials (i.e., government-issued ID, biometric checks, or liveness tests) before they are permitted to use a platform's services, ensuring that accounts can be linked to a real, identifiable individual**. This could be a relevant countermeasure against online financial scams in that it raises the cost and difficulty of creating fraudulent or anonymous accounts used to deceive victims and creates an accountability trail that may deter malicious actors.

This section solely focuses on identity verification requirements related to personal account creation. Know-Your-Business-Customer (KYBC) obligations, which refer to the onboarding of trader accounts, are discussed in a separate sub-section below.

This countermeasure is directly relevant to the risk factors associated with account creation and verification, and profile discovery and search ranking systems (Section 3.1.1). By requiring high-assurance identity verification, the measure directly addresses the risk that low barriers to account creation enable fraudsters to establish credible personas using false, stolen, or fabricated identities.

Information from designated services

The most consistent finding across the 2025 SRAs is that high-assurance identity verification is not required to create a personal account. Generally, sign-up requires only self-declared information (a name, email address or phone number, a password, and sometimes a date of birth) and confirmation by SMS or email. AliExpress, Amazon, Apple AppStore, Google's designated services, Snapchat, Shein, Temu, Zalando, and XNXX all follow this model.[721]

Facebook and Instagram report implementing a reactive identity verification process, triggered after account creation by a specific suspicious event rather than embedded in the registration process.[722] This verification functions primarily as an account recovery and abuse-response tool, rather than a mechanism to prevent inauthentic behaviour.

Some platforms report using automated behavioural and risk-scoring systems (LinkedIn's abuse risk scoring model, Facebook's and Instagram's classifiers for detecting previously removed actors).[723] Snapchat is also reportedly exploring third-party biometric tools for this purpose.[724] This approach prioritises accessibility in account creation, shifting the scam detection efforts to a post-registration monitoring phase that relies on detection measures, which are discussed in Section 5.2 below.

Analysis

The introduction of mandatory identity verification measures was extensively considered by Ofcom (UK communications service regulator) in relation to user-to-user platforms, under the framework of the Online Safety Act (OSA).[725] Those considerations are directly relevant to this section, given the similarities between the OSA and the DSA.

---

[721] AliExpress, Amazon, Apple AppStore, Google, Snapchat, Shein, Temu, Zalando, XNXX 2025 Systemic Risk Assessment Reports.

[722] Facebook, Instagram 2025 Systemic Risk Assessment Reports; Meta, Learn about ID verification for Meta accounts (2026), available at: https://www.meta.com/en-gb/help/quest/1266914157405903/?srsltid=AfmBOooDcIPBad4DpxMxhehVMlhwxWI2fEy1cor-kX6HO0RFB6XgPURy.

[723] LinkedIn, Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[724] Snapchat 2025 Systemic Risk Assessment Report.

[725] United Kingdom's Online Safety Act 2023 c.50 (2023), available at: https://www.legislation.gov.uk/ukpga/2023/50.

Identity verification measures refer to a broad range of methods, meant to ensure that the attributes claimed by a user do indeed belong to them. Lower assurance methods only require email addresses and/or telephone numbers – these are currently the most frequently used solutions, as described in the previous section. **Higher assurance methods require validation through government-issued documentation or other corroborative documentation linked to the user's identity**. It is argued that mandatory identity verification at account creation may deter users from sharing illegal or harmful content (such as scam content) online, and that it may make it harder for malicious actors to circumvent platform enforcement.[726]

However, Ofcom also notes that **high assurance identity validation methods can negatively impact users' right to privacy, and may have a chilling effect on their ability to exercise their rights to freedom of association and freedom of expression**.[727] This assessment is supported by a wide range of civil society organisations, which argue that the tools for digital identity verification may pose significant data protection risks.[728] Against this background, Ofcom concluded that mandatory high assurance identity verification measures at account creation are not a proportionate requirement to impose upon online platforms.[729]

Some stakeholders call for the introduction of **optional identity verification measures** that are free of charge for the users, arguing that this approach would offer a proportionate solution against the risks associated with anonymous or fake accounts, including online scams.[730] While users would still be able to create non-verified accounts,

---

[726] Ofcom, Protecting people from illegal harms online – Volume 4: How to mitigate the risk of illegal harms – the illegal content Codes of Practice (2023), available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/associated-documents/volume-4-how-to-mitigate-the-risk-of-illegal-harms--the-illegal-content-codes-of-practice?v=330398.

[727] ibid.

[728] Epicenter.works, Open Letter of Digital Rights and Consumer Organisations Concerning eIDAS Implementing Acts (2025), available at: https://epicenter.works/fileadmin/medienspiegel/user_upload/eIDAS_iAs_OpenLetter_2025.pdf; Electronic Frontier Foundation, Digital Identities and the Future of Age Verification in Europe (2025), available at: https://www.eff.org/deeplinks/2025/04/digital-identities-and-future-age-verification-europe; EDRi, Showing your ID to get online might become a reality – a closer look at the EU's new age verification app (2025), available at: https://edri.org/our-work/showing-your-id-to-get-online-might-become-a-reality-a-closer-look-at-the-eus-new-age-verification-app/.

[729] Ofcom, Protecting people from illegal harms online – Volume 4: How to mitigate the risk of illegal harms – the illegal content Codes of Practice (2023), available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/associated-documents/volume-4-how-to-mitigate-the-risk-of-illegal-harms--the-illegal-content-codes-of-practice?v=330398.

[730] Clean Up the Internet, Proposal for the inclusion, in the Illegal Harms Codes of Practice, of a measure requiring platforms to offer their users options to verify their identity (2024), available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/responses/clean-up-the-internet---proposal-for-a-measure-requiring-platforms-to-offer-their-users-options-to-verify-their-identity.pdf?v=370176; OneID, Response to Volume 3: How should services assess the risk of online harms? Consultation (2024), available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/responses/oneid-

the measure envisions that other users could see which accounts are verified or not, and even filter content to only see that posted by verified accounts. This measure is inspired by similar commitments under the Online Fraud Charter published by the UK Home Office, which identifies the choice to verify one's identity on platforms to allow other users to know they are genuine, in combination with allowing users to opt to interact with verified people only as an effective measure for tackling romance scams on dating platforms.[731] The introduction of this measure could be facilitated through the **European Digital Identity Wallet framework**, which is designed as a privacy-preserving, user-controlled model that allows for selective disclosure.[732]

A stricter scope of this measure, which was ultimately recommended by Ofcom, refers to the **introduction of identity verification measures for 'notable user' schemes or 'monetised labelling' schemes**.[733] These are schemes by which an online platform labels user profiles to indicate to other users they are 'notable' (e.g., politicians, celebrities, financial advisors, companies, government institutions); under 'monetised labelling' schemes, the label is available to any user that is willing to pay for it, irrespective of whether they qualify as 'notable'. As part of the identity verification measure for labelled accounts, platforms would adopt due diligence methods to ensure that the account is operated by or on behalf of the person it represents. This would entail verification at account creation, but also regular reviews to confirm whether the user profiles of relevant users continue to qualify to be labelled.

Behavioural studies show that the **labelled status positively influences users' trust towards the account and the content they post**.[734] As such, it is important to ensure that the identity behind these accounts is verified, to prevent the use of the labelling scheme to impersonate well-known figures to promote scam content, as was the case on X, where scammers took advantage of the monetised labelling scheme, which did not require identity verification, as part of their operations.[735] The European Commission has already fined X in relation to this function, which the Commission found to be deceptive

ltd.pdf?v=369998; South East Fermanagh Foundation, Response to Volume 3: How should services assess the risk of online harms? Consultation (2024), available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/responses/south-east-fermanagh-foundation.pdf?v=370014.

731 UK Home Office, Online Fraud Charter (2023), available at: https://assets.publishing.service.gov.uk/media/65688713cc1ec5000d8eef96/Online_Fraud_Charter_2023.pdf.

732 European Commission, European Digital Identity (EUDI) Regulation (2026), available at: https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation.

733 Ofcom, Illegal content Codes of Practice for user-to-user services (2025), available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-codes-of-practice-for-user-to-user-services-24-feb.pdf?v=391889.

734 Ofcom Behavioural Insights Team, User ID verification: What difference does a 'blue tick' make? (2025), available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/research-statistics-and-data/user-id-verification-what-difference-does-a-blue-tick-make/technical-report---ofcom-user-id-verification.pdf?v=399861.

735 Wired, Elon Musk's Twitter Is a Scammer's Paradise (2022), available at: https://www.wired.com/story/twitter-blue-check-verification-buy-scams/.

to users and to facilitate their exposure to scams.[736] It must be noted that the decision may be subject to appeal.

It is important to note that, despite the high-assurance character of the proposed identity verification measures, scammers may still circumvent them, particularly through hijacking legitimate accounts or using mule accounts. However, given that this measure is not widely implemented, aggregated data on the dimension of the risk of circumvention is not available yet.

Measure 2: KYBC requirements

General overview

KYBC requirements refer to **trader traceability measures, which verify the existence, legitimacy, registration, control, representatives, and commercial traceability of a business**. The implementation of these measures is mandated by Article 30 DSA for online platforms that allow consumers to conclude distance contracts with traders. Before a trader can offer products or services to EU consumers, the platform provider must collect key identification details, including contact details, identification documentation or electronic identification, payment account details, trade register information where applicable, and a self-certification of compliance with EU law.[737] The platform provider is required to make best efforts to assess whether this information is reliable and complete.[738] Moreover, the platform provider is also required to make this information available to its users in a clear and easily accessible manner.[739]

In practice, these measures can act as a countermeasure against online financial scams by making sellers more traceable, reducing the ability of fraudulent traders to re-enter under new identities, and supporting enforcement or consumer notification where illegal products or services are identified. The obligation to provide this information to individual users also plays a relevant role in increasing consumer awareness, allowing them to make informed decisions as to the goods and services they acquire.

This countermeasure is directly relevant to the risk factors of account creation and verification for business accounts and e-commerce integration (Section 3.1.1). KYBC requirements directly address risks arising from inadequate trader verification on marketplace platforms, where fraudulent sellers exploit weak onboarding processes to list non-existent products, counterfeit goods, or deceptive services.

[736] European Commission, Commission Decision of 5.12.2025 pursuant to Articles 73(1), 73(3) and 74(1) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) Cases DSA.100101, DSA.100102 and DSA.100103 – X (formerly Twitter) (2025), available at: https://ec.europa.eu/newsroom/dae/redirection/document/128762.

[737] Article 30(1) Digital Services Act.

[738] Article 30(2) Digital Services Act.

[739] Article 30(7) Digital Services Act.

Information from designated services

The most immediate finding of the review of 2025 SRAs is that KYBC obligations are only implemented by a subset of the designated services, specifically those that allow consumers to conclude distance contracts with traders.

Among the platforms to which KYBC obligations do apply, there is a notable degree of convergence on the core components of trader verification. All relevant platforms (AliExpress, Amazon, Apple AppStore, Booking.com, Shein, Temu, TikTok, and Zalando) collect broadly similar categories of information: business registration documents, legal representative identification, tax or VAT details, payment account information, and contact details.[740]

A consistent pattern across marketplace platforms is the use of layered verification combining automated screening with human review. Amazon combines automated forgery detection and image/audio verification with in-person or live video checks.[741] Apple uses automated hashing to detect duplicate accounts alongside human screening by its World Wide Developer Relations team.[742] Temu's system performs automated analysis for irregularities before escalating to manual review where inconsistencies are found.[743] AliExpress similarly uses an automated vetting system.[744] This layered approach reflects a recognition that purely automated systems may not be sufficient to detect sophisticated fraud, while purely manual review is not scalable.

A recurring feature across platforms is the use of blocklists to prevent previously removed or sanctioned traders from re-entering the platform under a new identity. AliExpress enforces this by comparing new applicants against banned sellers and restricting re-registration by terminated legal entities.[745] Apple cross-checks new developers against terminated accounts.[746] TikTok maintains explicit block lists for sellers removed for fraud or repeated violations.[747] Temu goes furthest, maintaining both an internal blocklist aggregating international sanctions lists and a separate onboarding restriction list for rogue traders.[748] This pattern reflects a shared recognition that point-in-time onboarding verification is insufficient without mechanisms to prevent circumvention through re-registration.

Some platforms go beyond onboarding verification to implement ongoing monitoring of trader information. Temu stands out as the most explicit example, requiring traders to update records as details change or expire, with suspension as the consequence for

---

[740] AliExpress, Amazon, Apple AppStore, Booking.com, Shein, Temu, TikTok, and Zalando 2025 Systemic Risk Assessment Reports.

[741] Amazon 2025 Systemic Risk Assessment Report.

[742] Apple AppStore 2025 Systemic Risk Assessment Report.

[743] Temu 2025 Systemic Risk Assessment Report.

[744] AliExpress 2025 Systemic Risk Assessment Report.

[745] ibid.

[746] Apple AppStore 2025 Systemic Risk Assessment Report.

[747] TikTok 2025 Systemic Risk Assessment Report.

[748] Temu 2025 Systemic Risk Assessment Report.

non-compliance.[749] Shein similarly verifies changes to seller information in real time.[750] By contrast, the 2025 Independent Audit of Booking.com specifically recommended introducing a monitoring system with periodic manual reviews – this finding highlights that continuous monitoring is not yet universal.[751]

Analysis

KYBC obligations operate as front-line gatekeeping mechanisms that seek to deny fraudsters the anonymity and pseudo-legitimacy on which scams depend. In the financial sector, regulators and institutions have long deployed Know Your Customer (KYC) protocols as one of the principal compliance tools for curbing fraudulent activity.[752] In the context of financial services, this control measure is generally recognised as a fundamental function preventing bad actors from registering, accessing and controlling mule accounts remotely.[753]

The logic of KYC processes has translated into the e-commerce environment, as observed in the trader-traceability regime of Article 30 DSA.[754] Even before this requirement was laid down in the DSA, a consultation carried out by the OECD with online marketplace providers confirmed that some operators already had implemented such controls in practice, with one marketplace requiring third-party sellers to undergo an anti-money-laundering (AML) and KYBC process through a third-party provider that recommends within two to three days whether the seller should be admitted, and others verifying seller identity details specifically to satisfy applicable AML and counter-terrorism-financing laws.[755] Online marketplaces that onboard business sellers typically demand proof of identity, contact information, tax-identification and trade-register numbers, and, in some cases, supporting documents and licensing.[756]

Upon testing the registration processes of ten online marketplaces (including the designated VLOP e-commerce platforms), vzbv reported that, in its opinion, they were

[749] ibid.

[750] Shein 2025 Systemic Risk Assessment Report.

[751] Deloitte, Booking.com B.V. Digital Services Act (DSA) Assurance Report, available at: https://www.dropbox.com/scl/fi/pct8bi29kykqq1tda58ct/2025-Audit-report.pdf?rlkey=t3mjd9dqmuer2rx4em6fyswwk&st=b7ohtnyo&e=1&dl=0.

[752] Consumers International, Stopping Online Scams: Building Consistency and Coordination for Consumers (2026), available at: https://www.consumersinternational.org/media/699948/consumers-international-stopping-online-scams-building-consistency-and-coordination-for-consumers.pdf; Interview 15.

[753] OECD, Protecting Consumers from Financial Scams and Frauds (2026), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/protecting-consumers-from-financial-scams-and-frauds_3887b249/d41817bb-en.pdf; FATF, Interpol and Egmont Group, Illicit Financial Flows from Cyber-Enabled Fraud (2023), available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf.

[754] Article 30, Digital Services Act.

[755] OECD, The Role of Online Marketplaces in Protecting and Empowering Consumers (2022), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/07/the-role-of-online-marketplaces-in-protecting-and-empowering-consumers_07af735e/9d8cc586-en.pdf.

[756] ibid.

'quite thorough,' with none of the cases permitting registration on incomplete details, and with submitted data assessed for completeness and plausibility before activation.[757] A generally favourable perspective on the KYBC processes implemented by e-commerce platforms was also expressed during the stakeholder consultation by one interviewee; however, it was noted **that the restrictiveness of these processes varies depending on the service and what they offer**.[758]

Despite this generally favourable outlook, the literature also notes gaps in implementation, enforcement and scope. Firstly, the scope of the trader traceability obligation is limited to online platforms allowing consumers to conclude distance contracts with traders. However, as noted by the OECD, **online scams are often also disseminated on consumer-to-consumer platforms that do not intermediate payment**.[759] These platforms allow registration with only a name and email address, which limits the ability of the service provider to ensure that third-party sellers it has previously sanctioned cannot re-register under a new alias.[760] Moreover, as no detailed identity information is collected, authorities encounter difficulties in using the marketplace's data to contact allegedly fraudulent third-party sellers.[761] These limitations are tied to the identity verification requirements described above, under Measure 1.

Secondly, vzbv reports that, in its opinion, the information displayed by the platforms it investigated does not match the requirements of the trader traceability obligation. The consumer organisation claims that while registration data is collected, it is, in its opinion, frequently not made meaningfully available to users or verified by the platform. Moreover, vzbv also claims that none of the thirty product pages it analysed displayed all the obligatory information, and that trader contact details were often missing, contradictory, or rendered as undecipherable transliterations, with out-of-date addresses.[762] The provision of this data is, however, important for consumers, as it allows them to individually assess whether the trader is legitimate.

A structural limitation of KYBC controls can be inferred from the implementation of KYC processes in the financial sector: **verification is often concentrated at onboarding while fraud migrates downstream**. For example, in the financial sector, it is reported by Sumsub that 76% of fraud attempts occur after the KYC process during day-to-day account use.[763] Verification is further eroded from both the supply and demand sides of identity: on one side, criminals deploy stolen, falsified, and synthetic identities; on the

[757] vzbv, Due Diligence Obligations of Online Marketplaces: A study on the implementation of Articles 30 and 31 of the Digital Services Act (DSA) (2025), available at: https://www.vzbv.de/sites/default/files/2025-11/25-06-17_MB-Report_Due_diligence_obligations.pdf.

[758] Interview 12.

[759] OECD, The Role of Online Marketplaces in Protecting and Empowering Consumers (2022), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/07/the-role-of-online-marketplaces-in-protecting-and-empowering-consumers_07af735e/9d8cc586-en.pdf.

[760] ibid.

[761] ibid.

[762] vzbv, Due Diligence Obligations of Online Marketplaces: A study on the implementation of Articles 30 and 31 of the Digital Services Act (DSA) (2025), available at: https://www.vzbv.de/sites/default/files/2025-11/25-06-17_MB-Report_Due_diligence_obligations.pdf.

[763] Sumsub, Identity Fraud Report 2024 (2024), available at: https://sumsub.com/fraud-report-2024/.

other, individuals are increasingly willing to sell their own KYC credentials, giving fraudsters a route to circumvent verification entirely.[764]

When translated into the e-commerce context, these findings indicate that **scammers would be able to circumvent KYBC processes by using false business registration documents.** Given the cross-border nature of e-commerce, identity checks cannot always be validated against government databases for sellers based abroad, which facilitates scammers' circumvention of KYBC processes through the use of fabricated documents.[765] Scammers also increasingly take over pre-existing, legitimate trader accounts, as reported by an interviewee; this behaviour mirrors the use of mule accounts in the financial sector.[766]

To address these deficiencies, the literature converges on a shift from one-off, onboarding-centred checks toward layered, risk-based, and continuously monitored verification, reinforced by stronger accountability and data-sharing. The OECD survey proposes requiring unique product identifiers and safety certification to aid traceability, while cautioning that additional screening should be risk-based and calibrated to objective criteria such as country of origin or product category to avoid disproportionate burden.[767]

Measure 3: Ad placement requirements

General overview

Ad placement requirements refer to **the conditions, verification processes, and content standards that platforms impose on advertisers before and after their advertisements are published**. Ad placement controls operate across two broad dimensions: who is permitted to advertise (identity and eligibility verification) and what they are permitted to advertise (content standards and moderation). Both dimensions are relevant to scam prevention.

The regulatory landscape governing online advertising in the context of financial scams is fragmented but expanding, and the line between mandatory obligations and voluntary commitments is not always clearly drawn in online platforms' own reporting. The DSA itself does not prescribe specific ad placement measures; however, Article 26 DSA requires platforms to ensure that advertising is clearly labelled and that the identity of the advertiser is transparent to users. This creates a baseline transparency obligation that complements but does not fully substitute for upfront identity verification. Advertising

[764] FATF, Interpol and Egmont Group, Illicit Financial Flows from Cyber-Enabled Fraud (2023), available at: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf.coredownload.inline.pdf.

[765] Examples of fabricated documents include incorporation or registration certificates, ID photos, bank statements; OECD, The Role of Online Marketplaces in Protecting and Empowering Consumers (2022), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/07/the-role-of-online-marketplaces-in-protecting-and-empowering-consumers_07af735e/9d8cc586-en.pdf;.

[766] Interview 12.

[767] OECD, The Role of Online Marketplaces in Protecting and Empowering Consumers (2022), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/07/the-role-of-online-marketplaces-in-protecting-and-empowering-consumers_07af735e/9d8cc586-en.pdf.

content is regulated largely through the Unfair Commercial Practices Directive (Directive 2005/29/EC), which is complemented by sector-specific rules, such as the EU's financial services regulatory framework (e.g., Markets in Financial Instruments Directive (Directive 2014/65/EU)), Consumer Credit Directive (Directive 2008/48/EC), or the upcoming Payment Services Regulation.[768] Specific rules on advertising are also imposed under the Audiovisual Media Services Directive (Directive 2010/13, as amended by Directive 2018/1808) or the Transparency and Targeting of Political Advertising Regulation (Regulation 2024/900).[769]

This countermeasure is directly relevant to the risk factor of advertising systems (Section 3.1.1), which the report identifies as a primary vector for the dissemination of scam content across VLOPs and VLOSEs. Ad placement requirements directly address risks arising from programmatic advertising infrastructure that enables fraudulent advertisements to reach large audiences through the same targeting mechanisms available to legitimate advertisers.

Information from designated services

The most striking finding resulting from the review of the 2025 SRAs is that explicit identity verification of advertisers prior to running ads is rare. Of the platforms that host advertising, only a handful implement structured advertiser identity verification as a distinct requirement. Bing stands out most clearly, with a dedicated Advertiser Identity Verification (AIV) process requiring advertisers to prove their legal identity before running ads.[770] Pinterest verifies merchants placing shopping ads.[771] Zalando and Amazon integrate advertiser verification into their broader KYBC process.[772] X requires an active X Premium subscription to run ads, with ID verification required for all creators receiving funds through Ad Revenue Sharing.[773] XNXX operates an Advertisers Certification Program requiring eligibility criteria, formal assessment, and periodic compliance

[768] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (2005), available at: https://eur-lex.europa.eu/eli/dir/2005/29/oj/eng; Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (2014), available at: https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng; Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (2008), available at: https://eur-lex.europa.eu/eli/dir/2008/48/oj/eng.

[769] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (consolidated text), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010L0013-20250208; Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (2024), available at: https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng.

[770] Bing 2025 Systemic Risk Assessment Report.

[771] Pinterest 2025 Systemic Risk Assessment Report.

[772] Amazon, Zalando 2025 Systemic Risk Assessment Reports.

[773] X 2025 Systemic Risk Assessment Report; X Help Center, ID Verification Policy & Privacy, available at: https://help.x.com/en/rules-and-policies/verification-policy.

reviews.[774] TikTok may require advertisers to submit documents to verify that their business or organisation is eligible to advertise on the platform.[775] For the rest of the platforms hosting advertisements (AliExpress, Apple AppStore, LinkedIn, Snapchat, Pornhub, XVideos, and X), no specific identity verification measures were reported in the 2025 SRAs. Google and Meta previously imposed additional identity verification across their services specifically for advertisers running ads on social issues, elections, or politics; however, both providers have since banned such ads on their platforms in Europe.[776]

Across virtually all designated services, the dominant approach to ad integrity is content moderation. Pre-publication automated review is near-universal, present in some form at AliExpress, Amazon, Apple AppStore, Bing, Facebook and Instagram, Google's designated services, LinkedIn, Snapchat, TikTok, X, XNXX, XVideos, and Pornhub.[777] The combination of automated review supplemented by human moderation is the sector's standard operating model.

A smaller number of platforms go beyond content review to implement risk-based or behavioural modelling at the advertiser account level. In the SRAs, Bing provides most details on its approach, which incorporates payment fraud detection triggered at the point of adding a payment instrument, a purchase risk model at billing, a behavioural risk model assessing account structure and campaign characteristics, and an LLM-based spoofing detection model targeting impersonation of legitimate sites such as banks.[778] Amazon reports that it proactively detects advertisers breaching its policies and uses audit findings to improve automated tools.[779] Facebook's and Instagram's automated systems analyse ads before they go live and apply reactive review post-publication based on user reports.[780] These more sophisticated approaches reflect a recognition that fraudulent advertisers adapt their content, making static content rules insufficient on their own.

Many platforms impose heightened requirements for specific high-risk advertising categories, even where general advertiser identity verification is absent. Google's designated services, LinkedIn, Pinterest, TikTok, and Bing all restrict or require certifications for categories such as financial services, healthcare, gambling, alcohol, and political content.[781] Meta's Special Ad Categories impose additional constraints on

[774] XNXX 2025 Systemic Risk Assessment Report.

[775] TikTok Business Resource Center, Advertiser Account Policy (2025), available at: https://ads.tiktok.com/resources/help/article/actor-policy.

[776] Google, Facebook and Instagram 2025 Systemic Risk Assessment Reports; Meta, Ending Political, Electoral and Social Issue Advertising in the EU in Response to Incoming European Regulation (2025), available at: https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/; Google Support, Update to Political Content Policy (2025), available at: https://support.google.com/adspolicy/answer/16409999?hl=en.

[777] AliExpress, Amazon, Apple AppStore, Bing, Facebook and Instagram, Google, LinkedIn, Pornhub, Snapchat, TikTok, X, XNXX, XVideos 2025 Systemic Risk Assessment Reports.

[778] Bing 2025 Systemic Risk Assessment Report.

[779] Amazon 2025 Systemic Risk Assessment Report.

[780] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[781] Bing, Google, LinkedIn, Pinterest, TikTok 2025 Systemic Risk Assessment Reports.

financial products advertising.[782] Apple requires proof of permits or licences for certain app categories, such as finance, healthcare, gambling, and legal services-related apps.[783] This category-based approach represents a partial, targeted form of identity or credential verification, but it is narrower in scope than universal advertiser verification and may still leave gaps where scam advertising falls outside the defined restricted categories.

Almost all advertising platforms include user reporting mechanisms as a reactive layer. Bing, Facebook, Google's designated services, Instagram, LinkedIn, Snapchat, TikTok, X, XNXX, XVideos, and Pornhub all allow users to flag potentially violative or fraudulent ads.[784] While user reporting provides a valuable signal, it is reactive by design, as it depends on a victim or observer identifying and reporting a problem after an ad has already been served.

Analysis

As a countermeasure against online financial scams, ad placement control measures entail a layered system that fulfils both prevention and detection functions. This understanding of ad placement controls mirrors recommendations from Consumers International, whose Global Action Agenda calls on platforms to prevent scam content by verifying advertisers, pre-approving listings, and swiftly removing scam content when it appears.[785]

As detailed in Section 3.1 of this report, shortcomings in identity verification mechanisms are a main risk factor associated with the advertising systems of online platforms. For example, a Reuters investigation alleges that Meta's internal documents would indicate that 'unverified advertisers are disproportionately responsible for harm on Meta's platforms'.[786] This information could not be independently verfieid by the study team. To address this risk, stakeholders call for **higher assurance identity verification measures for advertisers**.[787]

Amongst these calls, reference is often made to the enhanced transparency requirements implemented by some designated services pursuant to the Regulation on Transparency and Targeting of Political Advertising (TTPA Regulation).[788] These higher assurance methods commonly required submission of identity documents and liveness

[782] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[783] Apple AppStore 2025 Systemic Risk Assessment Report.

[784] Bing, Facebook, Google, Instagram, LinkedIn, Pornhub, Snapchat, TikTok, X, XNXX, XVideos 2025 Systemic Risk Assessment Reports.

[785] Consumers International, Protecting Consumers from Online Scams: A Global Action Agenda (2025), available at: https://www.consumersinternational.org/media/675471/consumers-international-global-action-agenda-to-protect-consumers-from-online-scams.pdf.

[786] Reuters, Meta created 'playbook' to fend off pressure to crack down on scammers, documents show (2026), available at: https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/.

[787] Interviews 4, 5, 14.

[788] Interviews 4, 5, 14.

checks.[789] However, as noted above, both Meta and Google have since prohibited political ads on their services.

Stakeholders interviewed have also highlighted that **additional verification requirements, including proof of regulatory authorisation, are required for actors placing ads related to regulated environments (e.g., financial services, gambling or pharmaceuticals)**.[790] One interviewee has highlighted that Google has introduced a financial services advertiser verification system across all its services; this process explicitly requires information about the entity's registration number and licence to provide financial services, which are **cross-checked against the relevant financial services registry** by an external compliance partner (G2RS).[791] This system was first introduced in the UK in 2021, and further expanded to almost 20 countries, including 6 EU Member States, namely France, Germany, Ireland, Italy, Portugal and Spain.[792] This countermeasure was strongly recommended by the respective stakeholder.[793]

This recommendation is mirrored by the guidelines published by the International Organisation of Securities Commissions (IOSCO), which calls on platforms 'to ensure that entities seeking to advertise paid content on their platforms are legally authorised to operate in the targeted jurisdictions and are not the subject of investor warnings by regulators', by cross-checking against I-SCAN, the global database of unlicensed firms providing investment services or engaging in illegal financial activities.[794]

High assurance identity verification measures have already been introduced in Singapore and Taiwan since 2024 and 2025, respectively. The Reuters investigation cited above alleges that Meta's internal testing documentation would indicate that verification measures introduced in Singapore and Taiwan immediately reduced scam ads in those countries by as much as 29%.[795]

[789] On Meta, see 'Confirm your identity to run ads about social issues, elections or politics', available at: https://www.facebook.com/business/help/2992964394067299?id=288762101909005; on Google, see 'Apply for Election Ads verification', available at: https://support.google.com/adspolicy/troubleshooter/9973345?hl=en.

[790] Interviews 4, 10.

[791] Interview 4; Google, Financial Services Verification: Relevant Regulators and Enforcement Dates, available at: https://support.google.com/adspolicy/answer/12390454?hl=en.

[792] Google, Financial Services Verification, available at: https://support.google.com/adspolicy/answer/15332527?hl=en&co=GENIE.CountryCode%3DFR&sjid=8981280511444481957-EU.

[793] Interview 4.

[794] IOSCO, IOSCO's Statement on Combating Online Harm and the Role of Platform Providers (2025), available at: https://www.iosco.org/news/pdf/IOSCONEWS770.pdf.

[795] Reuters, Meta created 'playbook' to fend off pressure to crack down on scammers, documents show (2026), available at: https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/.

In Singapore, a pilot programme requiring Meta and Carousell[796] to verify the identity of advertisers using identity documentation (Singpass[797]) and liveness checks is currently underway. In the context of the pilot programme, Meta has pledged to verify the identity of all advertisers placing ads on Facebook in Singapore.[798] On Carousell, the introduction of these measures has led to a 9% increase in the number of reported e-commerce scams between April and June 2025 compared to the same period last year; however, the measures also led to a 36% decrease in the total reported scams on Carousell for the same timeline comparison.[799] The effectiveness of the pilot programme is currently still under review.[800]

In Taiwan, platforms are required to verify the identity of advertisers through digital signature, rapid authentication system, or other technologies or methods with equivalent safety under Article 30 of the Fraud Crime Hazard Prevention Act.[801] Since the entry into force of the obligation in 2025, **Taiwan's Ministry of Digital Affairs reported that the stricter regulations brought down rates of investment scam ads by 96% and identity impersonation ads by 94%.**[802]

In addition to identity verification, an analysis of the advertiser's history that observes the advertiser's pattern of behaviour over time could help identify suspicious actors.[803] Such **behavioural analysis** can also be used to detect forgery, bot activity, and connections

[796] Carousell is a Singaporean e-commerce marketplace that allows users to purchase and sell used goods via its online platform.

[797] Singpass (Singapore Personal Access) is Singapore's national digital identity system.

[798] Singapore Ministry of Home Affairs, Assessment of Carousell's and Meta's Enhanced Verification Measures Under the E-commerce Code of the Online Criminal Harms Act (2025), available at: https://www.mha.gov.sg/media-room/newsroom/assessment-of-carousell-and-meta-enhanced-verification-measures-under-the-e-commerce-code-of-the-online-criminal-harms-act/.

[799] Singapore Ministry of Home Affairs, Enhanced Verification Measures by Carousell Under the E-Commerce Code of the Online Criminal Harms Act (2025), available at: https://www.mha.gov.sg/media-room/newsroom/enhanced-verification-measures-by-carousell-under-the-e-commerce-code-of-the-online-criminal-harms-act/.

[800] Singapore Ministry of Home Affairs, Status of step-up measures to be implemented by Carousell and additional consumer protection measures against e-commerce scams (2026), available at: https://www.mha.gov.sg/media-room/newsroom/status-of-step-up-measures-to-be-implemented-by-carousell-and-additional-consumer-protection-measures-against-e-commerce-scams/.

[801] Taiwan Ministry of the Interior, Fraud Crime Hazard Prevention Act, available at: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=D0080226.

[802] Reuters, Meta created 'playbook' to fend off pressure to crack down on scammers, documents show (2026), available at: https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/.

[803] Interview 10; corroborated by International Chamber of Commerce and GASA, Best practices for combating scams in advertising (2026), available at: https://iccwbo.org/wp-content/uploads/sites/3/2026/06/2026_ICC_GASA_Best_Practices_for_Combating_Scams_in_Advertising_EN.pdf; European Board for Digital Services, Second Report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risk as well as mitigation measures (2026), available at: https://digital-strategy.ec.europa.eu/en/library/second-report-systemic-risks-very-large-online-platforms-and-search-engines-under-digital-services.

to known malicious actor networks.[804] Currently, the Tech Transparency Project claims, for example, that Meta allegedly allows repeat offenders to still advertise on its services, despite their previous ads having been removed for violating the company's policies.[805]

Interviewees have also suggested the **introduction of friction mechanisms for newly onboarded advertisers**, such as cool-down periods (i.e., a mandatory waiting period before a new advertiser account is allowed to place ads on the platform), or restrictions on the number of ads that can be placed by new accounts, or their reach.[806]

Control over the identity of advertisers is complemented by control over the content of the ad, through **pre- and post-publication review measures**. On its own, advertiser verification may not prevent the dissemination of fraudulent ads – for example, BEUC reports that it has identified fraudulent ads on Google's designated services that were posted by verified accounts.[807] In a similar vein, an interviewee indicated that, given the marginal costs for obtaining a phone number (for SMS-based verification) and scammers' access to document and facial-recognition forgery tools, identity verification measures are ineffective if not complemented by detection and moderation processes.[808]

Measures concerning the content of an ad include pre-publication review, post-publication monitoring with reviews triggered by changes in the content of the ad (applicable for example to dynamic ads), and notice-and-action mechanisms for users to report ads they consider to be fraudulent.[809] The relationship between human and automated intervention in ad moderation reflects a division of labour that has shifted progressively toward automation, with human review retained for specific high-risk decisions and as a quality control layer over automated systems. Automated systems handle the bulk of ad review at scale, checking content, URLs, landing pages, images, and targeting parameters against policy rules. Human review is used as an escalation layer for cases that automated systems flag as uncertain or high-risk, or as a training and quality assurance function, with human reviewers generating labelled data that improves automated model performance over time. The functioning of these processes is analysed in detail in Section 5.2 below.

Generally, interviewed stakeholders and the literature recommend **a shift in efforts from reactive ad moderation to proactive review processes**, calling on service providers to take more measures to check, review and remove clusters of fraudulent ads (e.g., duplicate or very similar ads, ads posted by duplicate accounts, ads posted by the same account) once they become aware of the presence of a fraudulent ad on their

[804] ibid.

[805] Tech Transparency Project, Meta Awash in Deepfake Scam Ads (2025), available at: https://www.techtransparencyproject.org/articles/meta-awash-in-deepfake-scam-ads.

[806] Interviews 6, 10.

[807] BEUC, Sponsored by Scammers (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf.

[808] Interview 14.

[809] Interview 10.

service.[810] This would entail cross-checking the content of the ads available on their service, and the identity of the advertiser behind them, against any ad that was identified as fraudulent or violative (either pursuant to its own detection measures, or as flagged by users, including trusted flaggers).

Measure 4: Labelling AI-generated content

General overview

AI labelling (also referred to as AI content marking, watermarking, or transparency labelling) encompasses a set of technical and organisational measures designed to ensure that **AI-generated or AI-manipulated content, including deepfakes, synthetic text, and manipulated audio-visual material, is identifiable as such by both machines and humans.** In the context of online financial scams, AI labelling targets the use of deepfakes and synthetic content to impersonate real individuals, fabricate endorsements, create fake investment platforms, and deceive victims into making financial transfers.

The measures operate at two levels: **machine-readable marking** (invisible watermarks, metadata, cryptographic signatures embedded in AI-generated output, or lack of hardware-based noise patterns) and **human-perceptible labelling** (visible icons, banners, disclaimers, or auditory cues that alert viewers that content is AI-generated). Together, these mechanisms aim to break the chain of deception by making it harder for fraudsters to pass off AI-generated material as authentic.

This countermeasure is primarily relevant to the risk factor of AI-generated content as an operational amplifier (Section 3.2.3), addressing the growing use of deepfakes, synthetic media, and AI-generated text to impersonate trusted individuals, fabricate endorsements, and create fraudulent investment platforms.

Information from designated services

Among platforms that have taken steps to detect and label AI-generated content, some common approaches are taking shape, though they remain uneven in depth and sophistication. The most widespread measure is visible labelling: Bing, Facebook, Google's designated services, Instagram, LinkedIn, Pinterest, Snapchat, and TikTok all deploy some form of user-facing indicator (icons, textual labels, disclaimers, or context cards) to signal that content was generated or altered by AI.[811] This suggests an emerging norm that users should, at minimum, be informed when they encounter AI-produced material, even if platforms differ on how prominently that information is surfaced.

Underpinning several of these labelling efforts is a growing reliance on shared technical infrastructure, most notably the Coalition for Content Provenance and Authenticity

[810] Interviews 4, 5, 6; Reset Tech, Clickbait Cures: Unmasking the Deceptive Health Ad Infrastructure on Meta and Google (2026), available at: https://www.reset.tech/resources/reset-tech-clickbait-cures-unmasking-the-deceptive-health-ad-infrastructure-on-meta-and-google-april-2026-web.pdf.

[811] Bing, Facebook, Google, Instagram, LinkedIn, Pinterest, Snapchat, and TikTok 2025 Systemic Risk Assessment Reports.

(C2PA) standard. Bing, Google's designated services, LinkedIn, and TikTok all reference C2PA as a mechanism for embedding tamper-resistant metadata into content, enabling tracing of its origin and any AI involvement.[812] The adoption of a common provenance standard points to an industry-level recognition of the importance of interoperable solutions that travel with the content across ecosystems.

Watermarking reinforces this provenance logic at a more technical level. Bing applies a pixel-based watermark and content credentials to generated images, Google's designated services use SynthID (an imperceptible digital watermark spanning images, text, audio, and video), and Snapchat applies visible watermarks to exported AI-generated images.[813] These technologies are designed to embed a durable, traceable signal into the content itself so that its AI origin can be identified even after the content circulates beyond the platform where it was created.

Platforms have also moved to ensure that content generated by their own AI tools and shared on their services is systematically identified. Meta automatically labels photorealistic images created with MetaAI, TikTok labels content made with its AI effects, and Snapchat displays sparkle icons alongside AI-powered outputs.[814] This reflects a pragmatic starting point: platforms can most reliably identify and label content whose provenance they control from the point of creation. Yet it also reveals a limitation, since content generated by third-party AI tools or on other platforms falls outside this automatic identification layer.

To address that gap, several platforms have introduced creator disclosure obligations. TikTok provides tools for voluntary AI-content labelling, while YouTube requires creators to disclose realistic synthetic content and may apply a label itself when they fail to do so.[815] These mechanisms implicitly acknowledge that platform-side detection alone cannot capture all AI-generated content, and that creator responsibility must play a complementary role. However, the effectiveness of voluntary disclosure remains an open question.

Finally, a number of platforms integrate AI-generated content (AIGC) detection into their broader content moderation systems rather than treating it as a standalone function. Facebook and Instagram train their detection systems with synthetic data to improve performance against generative AI content.[816] TikTok reinforces AIGC detection through its existing moderation infrastructure, external partner reports, internal specialist teams, and targeted proactive sweeps.[817] LinkedIn uses computer vision and natural language processing to detect deepfakes in user profiles.[818] Pinterest and X apply their moderation tools to all harmful content regardless of how it was created, effectively treating AI

[812] Bing, Google, LinkedIn, TikTok 2025 Systemic Risk Assessment Reports.

[813] Bing, Google, Snapchat 2025 Systemic Risk Assessment Reports.

[814] Facebook, Instagram, Snapchat, TikTok 2025 Systemic Risk Assessment Reports.

[815] Google, TikTok 2025 Systemic Risk Assessment Reports.

[816] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[817] TikTok 2025 Systemic Risk Assessment Report.

[818] LinkedIn 2025 Systemic Risk Assessment Report.

generation as one vector among many rather than as a distinct category requiring separate treatment.[819]

A significant group of platforms (AliExpress, Amazon, Apple App Store, Booking.com, Pornhub, Shein, Temu, Wikipedia, X, XNXX, XVideos and Zalando) report no specific measures for detecting or labelling AI-generated content. Within this group, AliExpress and XVideos stand apart by acknowledging the necessity of further researching generative AI and developing detection algorithms, signalling awareness without implementation.[820] Apple addresses AI-generated content indirectly through its existing content guidelines and user-generated content controls rather than AI-specific mechanisms.[821] Pinterest occupies a middle ground: it labels content when metadata indicates AI involvement but does not otherwise treat AI-generated harmful content as a distinct category in its moderation processes.[822]

Analysis

AI labelling measures operate as transparency and accountability mechanisms designed to reduce the informational asymmetry that online scammers exploit when they use synthetic media to impersonate trusted persons, fabricate endorsements, or create false evidence of legitimacy.[823] This category of measures encompasses a sequential chain of events, from scanning and detection by online platforms of synthetic content to the implementation of interface design specifications that signal to users that the content they are engaging with has been generated or edited using AI.

In the EU framework, Article 50 of the AI Act requires providers of certain AI systems to ensure that AI-generated or manipulated content is marked in a machine-readable format and detectable as artificially generated or manipulated, while deployers of systems generating or manipulating deepfakes must disclose that the content has been artificially generated or manipulated.[824] The Commission's Code of Practice on marking and labelling AI-generated content further operationalises these obligations by distinguishing between provider-side measures, such as machine-readable marking and detection, and

[819] Pinterest, X 2025 Systemic Risk Assessment Reports.

[820] AliExpress, XVideos 2025 Systemic Risk Assessment Reports.

[821] Apple AppStore 2025 Systemic Risk Assessment Report.

[822] Pinterest 2025 Systemic Risk Assessment Report.

[823] NSA, ASD ACSC, CCCS and NCSC-UK, Content Credentials: Strengthening Multimedia Integrity in the Generative AI Era (2025), available at: https://media.defense.gov/2025/Jan/29/2003634788/-1/-1/0/CSI-CONTENT-CREDENTIALS.PDF; Center for News, Technology & Innovation, Synthetic Media & Deepfakes: How do we protect societies from synthetic media and "deepfakes"? (2025), available at: https://cnti.org/issue-primers/synthetic-media-deepfakes/;

[824] (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L2024/1689 (AI Act), available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng.

deployer-side measures, such as visible labelling of deepfakes and certain AI-generated text.[825]

In the scam context, the measures to be implemented under the AI Act framework may assist detection by giving platforms and investigators technical signals of synthetic origin, and prevention by warning users before they rely on fake investment videos, celebrity endorsements, or impersonation messages.

The literature, however, consistently cautions that labelling, watermarking, and provenance systems are not complete anti-scam solutions. **Technical limitations include the dependence of watermarking on upstream compliance by AI providers, the possibility that watermarks may be removed or degraded through compression, cropping, screenshots, re-encoding, or adversarial manipulation, and the lack of interoperability across proprietary marking systems**.[826]

The Coalition for Content Provenance and Authenticity ('C2PA') is the principal standards body developing a provenance infrastructure for media content. Its specifications define an opt-in technical architecture for attaching cryptographically signed 'Content Credentials' to digital assets so that downstream systems can verify assertions about origin, editing history, AI generation, and other provenance information.[827] As the initiative is organised as a coalition and standards ecosystem, the adoption of its guidelines remains voluntary – therefore, scammers revert to the use of open-source AI models, or other LLMs that do not adhere to the C2PA standards, to avoid the creation of watermarked content that can be detected by the platforms.

C2PA-style provenance systems raise a related but distinct set of issues: they can provide tamper-evident information about the origin and history of a digital asset, but they do not themselves determine whether content is fraudulent, whether a financial promotion is lawful, or whether an endorsement is authorised.[828]

Moreover, **AI labels may be ignored or misunderstood by users, especially where scams rely on urgency, emotional pressure, social proof, or paid amplification**.[829] Missing labels may also be wrongly perceived by users as proof of the authenticity of the

[825] European Commission, Code of Practice on Transparency of AI-Generated Content (2026), available at: https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content.

[826] Nikola Jovanovic et al., Watermark Stealing in Large Language Models (2024), available at: https://watermark-stealing.org/; Karanpartap Singh and James Zou, New Evaluation Metrics Capture Quality Degradation due to LLM Watermarking (2023), available at: https://arxiv.org/pdf/2312.02382; Mehrdad Saberi et al., Robustness of AI-Image Detectors: Fundamental Limits and Practical Attacks (2024), available at: https://arxiv.org/pdf/2310.00076.

[827] C2PA, The Content Authenticity Initiative: Setting the Standard for Digital Content Attribution (2020), available at: https://acrobat.adobe.com/link/track?uri=urn%3Aaaid%3Ascds%3AUS%3A2c6361d5-b8da-4aca-89bd-1ed66cd22d19.

[828] C2PA, C2PA Content Credentials Explained: Addressing Common Questions and Updates (2025), available at: https://c2pa.org/wp-content/uploads/sites/33/2025/10/content_credentials_wp_0925.pdf; Ofcom, Qualitative study: User perspectives on AI content labels (2025), available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/deepfake-defences-2/ai-content-labels-qualitative-research-report.pdf?v=399905.

[829] US National Institute of Standards and Technology (NIST), Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency (2024), available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-4.pdf.

content, rather than a shortcoming in the detection system.[830] For that reason, academic literature is exploring a new avenue for the use of labelling as a countermeasure: the development of labels that focus on the potential harm of content (e.g., 'manipulated' or 'deceptive') labels, in addition to provenance labels.[831] Similarly, the use of 'Readers/Users added context' labels is another approach that could allow users to better distinguish the scam intentions behind certain synthetic media, as tested by Ofcom.[832] While Ofcom's research identified that this type of label, which allows users to provide any information about a given post, is the only type of label tested by the institution that can directly alert users to the possibility of a scam deepfake, it also found that users expressed confusion and uncertainty as to the legitimacy of the claims under the label.[833]

In general, the use of AI labelling is a topic that requires further research, particularly in relation to the development of high-accuracy detection mechanisms. Given the novel character of this technology, AI labels should only be used as one signal in a broader risk-based scam counterstrategy.

5.2. Detection and removal measures

Detection and removal measures constitute an interrelated set of platform countermeasures encompassing automated detection systems, human review processes, and removal or restriction actions as well as the detection of coordinated scam activity and recommender system safeguards. These countermeasures operate as dynamic and interdependent components of a broader enforcement chain, where signals generated at one stage inform and reinforce actions at others.

Measure 1: Automated detection systems

General overview

The use of automated detection systems is among the **most common countermeasures** employed by online platforms to assess whether content or actors exhibit potentially malicious intent. These systems are based on URL and domain reputation analysis, as well as advanced machine learning and AI-based systems capable of identifying scams based on a range of textual, visual, behavioural and contextual signals.[834] Further technologies include large language models (LLMs) and deep learning models, which can review content at high volume while capturing more

[830] ibid.

[831] Chloe Wittenberg et al., Labeling AI-Generated Content: Promises, Perils, and Future Directions (2023), available at: https://computing.mit.edu/wp-content/uploads/2023/11/AI-Policy_Labeling.pdf.

[832] Ofcom, Qualitative study: User perspectives on AI content labels (2025), available at: https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/deepfake-defences-2/ai-content-labels-qualitative-research-report.pdf?v=399905.

[833] ibid.

[834] Interview 12,13.

nuances and reasoning across complex questions and cases.[835] In practice, these systems can therefore act as a countermeasure against online financial scams by enabling the automated identification of potentially malicious content and actors at scale.

Platforms also use knowledge graph technology to relate relationships across accounts, transactions, and listings, as well as cluster mapping technology, which maps relationships across accounts, domains, infrastructure, and transactions to identify coordinated networks and attribute them to a single campaign.[836] Computer vision is also used to analyse the visual elements of suspected phishing sites and fraudulent content alongside textual signals and brand impersonation detection: as scammers shift toward visual deception and fake brand recreation, visual analysis is increasingly important.[837] These techniques operate in combination and enable automated identification of potential scams before and during user exposure. The importance of integrating multiple detection capabilities has increased considerably with the growth of AI-generated content. As a result, many platforms are moving beyond isolated forms towards multimodal detection systems capable of evaluating multiple types of information simultaneously rather than assessing individual signals in isolation.[838]

This countermeasure addresses multiple risk factors identified in Section 3.1.1, including advertising systems, account creation and verification, recommender systems, and e-commerce integration. Automated detection systems are designed to directly address risks arising from the scale and speed at which fraudulent content can be disseminated across designated services, including fraudulent advertisements, fake product listings, and scam profiles. By scanning content, URLs, landing pages, and behavioural signals, these systems partially address risks associated with platform features that enable rapid content distribution.

Information from designated services

Based on the 2025 SRAs, several common patterns emerge in how automated systems are deployed for content moderation and scam detection. Most platforms (AliExpress, Amazon, Bing, Facebook, Instagram, Shein, Temu, XNXX, and Xvideos) rely on fused image-and-text analysis to detect counterfeit goods, scams, or policy violations, reflecting an industry-wide shift away from single-modality detection.[839]

Fake review and rating manipulation is another near-universal concern, with AliExpress, Amazon, Google Shopping, Google Play and Google Maps, and Zalando all deploying systems that examine account linkages, sign-in behaviour, or reviewer network

[835] ibid.

[836] ibid.

[837] Interviews 12, 13.

[838] Interview 13.

[839] AliExpress, Amazon, Bing, Facebook, Instagram, Shein, Temu, XNXX, and Xvideos 2025 Systemic Risk Assessment Reports.

anomalies to catch coordinated manipulation.[840] Behavioural and anomaly-based scam detection is employed by Amazon, Shein, Temu, Snapchat, and TikTok.[841]

Alongside these commonalities, several platforms adopt unique approaches. For example, Amazon reports that its SENTRIX system, which scans suspicious URLs to detect malicious websites and URLs, extends beyond marketplace content to detect external phishing sites impersonating the brand, layering in third-party and human verification before takedown.[842] Facebook and Instagram describe a provenance-tracing capability that reverse-engineers AI-generated images and produces explainable reports for human reviewers.[843]

According to the DSA Transparency Database, since the beginning of 2025 around 53 million Statements of Reasons (SoRs) related to scams have been issued for content categorised as text where the moderation decision was fully automated or partially automated. Approximately 58% of these decisions originated from Google Maps, 26% from TikTok, and 12% from Amazon. The services listed in the table below are those that reported scam-related content removals in the DSA Transparency Database during the relevant period.

Table 6 - Textual content[844]

Designated services[845]	SoR (in thousands)
Google Maps	30.741
TikTok	14.084
Amazon	6.479
AliExpress	681
Temu	606
Facebook	363

According to the DSA Transparency Database, since the beginning of 2025 approximately 8.35 million SoRs related to scams have been issued for image and video content through fully or partially automated moderation processes. Approximately 44% originated from TikTok, 30% from Facebook, and 20% from Google Maps. The services listed in the table below are those that reported scam-related content removals in the DSA Transparency Database during the relevant period.

[840] AliExpress, Amazon, Google, and Zalando 2025 Systemic Risk Assessment Reports.

[841] Amazon, Shein, Temu, Snapchat, and TikTok 2025 Systemic Risk Assessment Reports.

[842] Amazon 2025 Systemic Risk Assessment Report.

[843] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[844] Accounted period: 01/01/2025-30/05/2026.

[845] Stripchat has been omitted from the list of VLOPs and VLOSEs by the European Commission in 2025 and is therefore not included in the table.

Table 7 - Image and video content[846]

Designated services	SoR (in thousands)
TikTok	3.686
Facebook	2.569
Google Maps	1.690
Temu	216
Google Shopping	79
Instagram	59
YouTube	44
Snapchat	3
Amazon	1

Analysis

While automated detection systems are widely recognised as necessary given the scale at which VLOPs and VLOSEs operate, they remain **vulnerable to a range of adaptive circumvention techniques** employed by scammers. One industry stakeholder estimated that the designated services manage to stop 95% of all scam attacks.[847] Nevertheless, even the small percentage of scams that reach their services may still represent substantial volumes of harmful content.[848]

An independent auditing study examining online scam-detection mechanisms on video-sharing platforms found that even comparatively advanced detection systems remained vulnerable to relatively simple evasion attacks, reporting that automated moderation systems continue to face significant limitations when confronted with adaptive circumvention strategies.[849] Scammers employ **a variety of evasion techniques to bypass automated detection mechanisms** by, for instance, deliberately misspelling flagged keywords, embedding text within images to avoid text matching, using audio distortions to circumvent audio analysis, and utilising generative AI to create unique variations of scam content that do not match existing content libraries.[850]

Another commonly identified evasion technique is **URL masking**, whereby advertisements display links that appear to originate from trusted brands or marketplaces while redirecting users to unrelated fraudulent websites. According to Gen Digital, Meta's advertising infrastructure may expose only the visible domain displayed within an advertisement rather than the final destination reached after clicking, making this form of

[846] Accounted period: 01/01/2025-30/05/2026.

[847] Interview 11.

[848] ibid.

[849] Miriam Marciel et al., Understanding the Detection of View Fraud in Video Content Portals (2016), available at: https://arxiv.org/pdf/1507.08874.

[850] ibid.

deception considerably more difficult for automated systems to identify.[851] The use of Unicode obfuscation, whereby scammers replace standard characters with visually similar alternatives, has also been identified by Gen Digital as a common evasion technique.[852] While the text remains understandable to human users, automated systems may struggle to interpret it correctly, particularly when combined with domain impersonation, celebrity references, or other deceptive signals.

Further, **scammers leverage linguistic and regional disparities in automated moderation performance**. A study by AI Forensics examining political advertisements across 16 EU Member States identified substantial linguistic variation between countries, with the researchers suggesting there may be uneven moderation effectiveness across languages and national contexts.[853] Ireland, the only English-speaking country included in the study, recorded the highest moderation recall, with 22.8% of undeclared political advertisements subsequently identified and moderated by the platform, compared with only 3.9% in Hungary.[854] Although the study focused on political advertising, the findings are relevant for online scams since automated detection systems rely on similar linguistic and machine-learning models. Further, scammers may exploit the use of technical terminology, coded expressions, or slang that can be more difficult for automated moderation systems to interpret accurately, particularly where effective classification depends on contextual understanding.[855]

Furthermore, the effectiveness of some platform automated detection systems has been questioned by third parties.[856] A distinct concern is whether platforms' automated detection systems effectively identify fraudulent advertisements in the first place. For example, on 30 April 2024, the European Commission opened formal investigation proceedings against Meta concerning deceptive advertisements on Facebook and Instagram that could lure users into financial scams.[857]

In a large-scale investigation across 13 Member States, BEUC documented 863 suspected fraudulent financial advertisements on Facebook, Instagram and TikTok, including advertisements promoting payday loans despite these platforms expressly prohibiting such advertisements under their advertising policies. While Facebook and Instagram rejected around 43% of the submissions against fraudulent ads, TikTok removed 21% of the submitted ads.[858] According to BEUC, in many cases, the

[851] Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll.

[852] ibid.

[853] AI Forensics, No Embargo in Sight (2025), available at: https://aiforensics.org/uploads/No_Embargo_in_Sight_AI_Forensics_Report.pdf.

[854] ibid.

[855] Multi-stakeholder Workshop on Online Financial Scams.

[856] Multi-stakeholder Workshop on Online Financial Scams.

[857] European Commission, Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act (2024), available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373

[858] European Consumer Organisation (BEUC), Sponsored by Scammers: How Big Tech Platforms Facilitate Financial Fraud (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf.

problematic nature of the advertisements appeared readily identifiable from the advertisement text itself; this finding led to questions from BEUC about the practical effectiveness of platform automated detection systems.[859] BEUC has also raised comparable concerns regarding Google's advertising ecosystem. On Google's designated services, consumer groups identified 30 examples of fraudulent advertisements that breached EU rules and/or Google's advertising policies; 60% of them were removed.[860] Although Google operates an advertiser verification programme through its ad library, BEUC claims that both verified and non-verified advertisers are able to publish and disseminate fraudulent advertisements.[861]

In addition, **third parties are concerned with platforms providing only limited information regarding the actual performance of their automated detection systems**, making independent evaluation difficult.[862] For example, according to FactReview, Meta states that it maintains a high level of accuracy and discloses an overall automation overturn rate of 7.47% across content categories.[863] However, FactReview argues that this metric provides only a partial indication of false positives and does not reveal the false-negative rate, namely the proportion of infringing scam-related content and advertisements that evade detection altogether.[864] Similarly, industry-standard performance measures such as precision and recall are generally not disclosed. Although Meta states that its systems are subject to random audits and continuous improvement, FactReview argues that the absence of detailed performance metrics limits meaningful assessment of whether automated systems effectively reduce scam-related risks in practice.[865]

More broadly, according to third parties, **the limited transparency surrounding platform detection systems makes it difficult to understand how automated enforcement is operationalised**, including the extent to which models specifically target scam advertisements, organic content, coordinated behaviour, or broader indicators of policy violations.[866] While some platforms publish general descriptions of their use of AI to combat scams, relatively little information is available regarding the design, functioning, or evaluation of the underlying detection models.[867] Commercial confidentiality, intellectual property considerations, and security concerns provide legitimate reasons for withholding detailed technical information, including model parameters and detection methodologies.[868] Nevertheless, greater transparency

[859] ibid.

[860] ibid.

[861] ibid.

[862] Multi-stakeholder Workshop on Online Financial Scams.

[863] FactReview, Special Trusted Flagger Report #1 (2025), available at: https://factreview.gr/2025/01/31/trusted-flagger-special-report-1-eng/.

[864] ibid.

[865] ibid.

[866] Multi-stakeholder Workshop on Online Financial Scams.

[867] ibid.

[868] Jun Niu et al., A survey on membership inference attacks and defenses in machine learning (2024), available at: https://www.sciencedirect.com/science/article/pii/S2949715924000064.

regarding the categories of signals used, the objectives of automated detection systems, the evaluation methodologies applied, and aggregate performance metrics would facilitate more meaningful independent scrutiny while avoiding disclosure of information that could enable malicious actors to circumvent platform enforcement.[869]

Measure 2: Human review

General overview

Alongside automated detection systems, human review and scam investigation teams constitute an important complementary layer of platform countermeasures against online financial scams. Human review remains particularly important for **complex, high-risk, or context-dependent cases**, where purely automated systems may face limitations.[870] Investigative teams also conduct proactive threat hunting by monitoring emerging scam typologies, high-risk keywords, suspicious URLs, and other indicators of abuse, thereby providing qualitative insights that complement automated detection. Human review is typically triggered following identification through automated detection systems, user reports, trusted flaggers, or internal investigations. It serves to verify potential violations, resolve ambiguous cases, and investigate high-risk scam operations. For many online platforms, human review functions both as a quality-control mechanism for automated moderation systems and as an independent investigative capability for scams that remain difficult to detect algorithmically.

This countermeasure complements automated detection and directly addresses the limitations of algorithmic systems in complex, context-dependent scam cases. Human review is relevant to risk factors associated with advertising systems, account creation and verification, and e-commerce integration (Section 3.1.1), where automated systems may generate ambiguous or high-risk signals requiring human judgment. The countermeasure partially addresses risks arising from sophisticated operational tools (Section 3.2.3), including deepfakes and AI-generated content, which may evade purely algorithmic detection.

Information from designated services

Based on the 2025 SRAs, human moderation functions as a secondary, contextual layer applied to content and activity already flagged by automated systems. Most platforms (Google's designated services, Shein, XNXX, Xvideos, Pinterest, and LinkedIn) follow a straightforward escalation model, where automated systems surface potential violations and human reviewers verify or contextualise them before enforcement.[871]

A number of platforms (Amazon, Bing, Facebook, Instagram) maintain specialist investigative teams focused on organised or networked abuse.[872] Several platforms also

[869] Sarah Lee, Detecting Bias in Machine Learning Models (2025), available at: https://www.numberanalytics.com/blog/ultimate-guide-bias-detection-machine-learning.

[870] Interview 12.

[871] Google, Shein, XNXX, Xvideos, Pinterest, and LinkedIn 2025 Systemic Risk Assessment Reports.

[872] Amazon, Bing, Facebook, Instagram 2025 Systemic Risk Assessment Reports.

describe non-escalation-based human review: AliExpress reports that it conducts routine sweeps and user-like searches for infringing products, X states that it performs periodic proactive sweeps alongside event-based monitoring, and Apple claims that it requires every app submission and update to undergo human review prior to publication regardless of automated flagging.[873]

TikTok, Facebook and Instagram describe human review as a check on AI outputs, with reviewers assessing the results of scam- or synthetic-media-detection systems before enforcement decisions are finalised.[874] Uniquely, Wikipedia relies on volunteer editors and administrators rather than an employed trust-and-safety function.[875]

Some SRAs (Booking.com, Pornhub, Zalando) describe dedicated review or investigation teams without providing detail on process, scale, or escalation criteria.[876]

Data from the DSA Transparency Database illustrates that human moderation is a significant component of platform enforcement despite increasing levels of automation. Considering SoRs related to scams that were issued without the use of automated detection or automated decision-making, approximately 4,6 million enforcement decisions were taken through fully human review processes since the beginning of 2025. The table below presents the distribution of these SoRs across designated services for which data are available. The largest share was reported by TikTok (44% of the total), followed by Facebook (33%), Snapchat (8%), and Instagram (8%). The services listed in the table are those that reported scam-related content removals in the DSA Transparency Database during the relevant period.

Table 8 - Scam-related human moderation[877]

Designated service	SoRs (in thousands)
TikTok	2.027
Facebook	1.543
Snapchat	375
Instagram	372
X	98
YouTube	79
Apple App Store	26
AliExpress	22
Pinterest	18
Booking.com	11

[873] AliExpress, Apple AppStore, X 2025 Systemic Risk Assessment Reports.

[874] Facebook, Instagram, TikTok 2025 Systemic Risk Assessment Reports.

[875] Wikipedia 2025 Systemic Risk Assessment Report.

[876] Booking.com, Pornhub, Zalando 2025 Systemic Risk Assessment Reports.

[877] Accounted period: 01/01/2025-30/05/2026.

Designated service	SoRs (in thousands)
LinkedIn	6
Google Play	2
Google Shopping	1
Shein	1
Temu	1
Zalando	1

Analysis

Despite the central role of human review in platform governance, third-party research, as cited below, highlights concerns regarding its transparency, capacity, and effectiveness.

A key concern is whether **human moderation capacity is proportionate to platform scale**.[878] According to the European Digital Media Observatory (EDMO), Meta employed 5,548 content moderators covering the 24 official languages of the EU between April and September 2024.[879] During the same period, Facebook alone reported approximately 260.6 million monthly active users within the EU.[880] This corresponds to approximately one moderator for every 47,000 monthly active Facebook users, before accounting for Instagram users, content volumes, advertisements, or reported material requiring review. The trusted flagger FactReview also noted significant variation in moderation coverage across Member States, with comparatively greater resources allocated to larger markets such as Germany and Italy and more limited coverage in smaller or less prioritised contexts.[881] A different but related concern is that scam identification frequently depends on contextual interpretation, which may make consistent human review more challenging, particularly where the deceptive nature of the content is not immediately apparent.[882]

Third parties also note that platforms provide relatively limited information regarding how human review operates in practice. According to FactReview, designated services do not disclose the proportion of user-reported content that ultimately receives human review, nor do they specify how many flagged advertisements are assessed by human moderators before enforcement decisions are taken.[883] In addition, the effectiveness of user reporting mechanisms may depend on the accessibility and design of reporting

[878] Multi-stakeholder Workshop on Online Financial Scams.

[879] European Digital Media Observatory (EDMO), Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU (2025), available at: https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.

[880] ibid.

[881] FactReview, Special Trusted Flagger Report #1 (2025), available at: https://factreview.gr/2025/01/31/trusted-flagger-special-report-1-eng/.

[882] Multi-stakeholder Workshop on Online Financial Scams.

[883] ibid.

interfaces, including the availability and clarity of reporting categories.[884] Where reporting options are overly narrow, unclear, or difficult for users to navigate, potentially harmful content may not be appropriately flagged or may be misclassified, limiting the ability of platforms to identify and review problematic content effectively. FactReview argues that public reporting instead focuses primarily on aggregate staffing figures, providing limited insight into how moderators are allocated across languages, content categories, or enforcement priorities.[885]

A further limitation identified by FactReview concerns the **lack of publicly available performance metrics relating to human review**. The trusted flagger noted that although designated services report continuous investment in moderation technologies and state that review teams operate on a 24/7 basis, no systematic information is published regarding the accuracy of automated assessments, the proportion of automated decisions subsequently reviewed by humans, or the share of user reports that receive human evaluation.[886] As a result, EDMO argues that important elements of the moderation pipeline remain opaque, including the interaction between automated and human enforcement, the effectiveness of escalation mechanisms, and the extent to which human review is capable of compensating for the known limitations of automated scam-detection systems.[887]

Measure 3: Removal and suspension mechanisms

General overview

Removal mechanisms constitute the final enforcement stage of scam countermeasures. Once a violation has been identified through automated detection, human review, or other investigative processes, **removal measures determine the consequences imposed on the offending content, account, or network**. These measures include, among others, content removal, advertisement rejection, application removal, review deletion, merchant restrictions, account suspension, permanent account termination, the addition of advertisers to blocklists to prevent re-registration, and the use of enforcement signals to proactively identify similar actors. In practice, these measures can act as a countermeasure against online financial scams by removing fraudulent content, imposing sanctions on the actors responsible, and dismantling broader scam infrastructures. Some platforms also pursue legal action against scammers and seek to disrupt scam infrastructure beyond their own services.[888] Conceptually, enforcement measures can operate at three levels. First, platforms may remove individual pieces of content, such as scam advertisements, listings, reviews, applications, or posts. Second, they may impose sanctions on the actors responsible, including advertisers, merchants, developers, or account holders. Third, platforms may seek to dismantle broader scam

[884] ibid.

[885] ibid.

[886] ibid.

[887] European Digital Media Observatory (EDMO), Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU (2025), available at: https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.

[888] Interview 12.

infrastructures by disrupting coordinated networks, advertiser ecosystems, and repeat-offender operations (discussed under Measure 4). The effectiveness of enforcement therefore depends not only on the volume of removals but also on the extent to which platforms prevent fraudulent actors from re-entering their services and continuing their activities.

This countermeasure directly addresses risks arising from account creation and verification (Section 3.1.1), insofar as removal and suspension mechanisms impose consequences on fraudulent accounts and advertisers. The measure is also partially relevant for risks associated with advertising systems and e-commerce integration by removing fraudulent advertisements and product listings.

Information from designated services

Based on the 2025 SRAs, enforcement mechanisms generally follow a graduated, severity-based logic, where content or accounts are removed, restricted, or escalated depending on the confidence and recurrence of detected violations, though the sophistication of these frameworks varies considerably. Several platforms employ explicit tiered or strike-based systems: Google's designated services apply a 'three-strikes' policy for repeated advertising violations, Temu operates a graduated three-tier enforcement structure culminating in permanent inclusion on a Trader Blocklist, and TikTok escalates from warnings to temporary suspensions and ultimately permanent termination.[889]

A common pattern also emerges around risk-scoring thresholds determining the enforcement pathway. Pinterest and LinkedIn both describe automated removal for high-confidence violations, with lower-confidence or medium-risk cases instead escalated for human review or subject to reduced distribution rather than outright removal.[890] Network-level and coordinated-abuse enforcement is another recurring theme among platforms, with Facebook, Instagram, Amazon, Snapchat and Bing reporting processes intended to detect coordinated inauthentic behaviour.[891]

Marketplace platforms (AliExpress, Amazon, Shein, Zalando, Booking.com) report combining listing-level removal with seller or host account suspension, while app platforms (Apple AppStore and Google Play) claim enforcement occurs at both the submission stage (pre-publication rejection) and post-publication stage (removal or account restriction).[892]

Data from the DSA Transparency Database illustrates the scale at which removal mechanisms are deployed. Between the designated services examined, since the beginning of 2025, approximately 128 million SoRs relating to scam-related content removals were issued. According to the table below, content removals were distributed across a relatively broad range of services, although a small number of platforms accounted for the majority of enforcement activity. YouTube alone accounted for approximately 49% of all recorded content removals, followed by Google Maps (27%),

[889] Google, Temu, TikTok 2025 Systemic Risk Assessment Reports.

[890] Pinterest, LinkedIn 2025 Systemic Risk Assessment Reports.

[891] Facebook, Instagram, Amazon, Snapchat, Bing 2025 Systemic Risk Assessment Reports.

[892] AliExpress, Amazon, Shein, Zalando, Booking.com, Apple AppStore, Google 2025 Systemic Risk Assessment Reports.

TikTok (14%), and Facebook (6%). The services listed in the table are those that reported scam-related content removals in the DSA Transparency Database during the relevant period.

Table 9 - Scam-related content removals[893]

Designated service	SoRs (in thousands)
YouTube	62.184
Google Maps	34.988
TikTok	17.543
Facebook	8.080
Google Shopping	2.378
Temu	833
Instagram	763
AliExpress	683
Snapchat	300
Google Play	44
Amazon	35
LinkedIn	25
Pinterest	24

Regarding account suspensions, the DSA Transparency Database records approximately 280 million suspensions, the overwhelming majority of which originated from Facebook. The platform accounted for approximately 99% of all recorded account suspensions, indicating a substantially greater reliance on account-level sanctions than other designated services. The services listed in the table below are those that reported scam-related account suspensions in the DSA Transparency Database during the relevant period.

Table 10 - Scam-related account suspensions[894]

Designated service[895]	SoRs (in thousands)
Facebook	277.911
Amazon	1.133
X	818
AliExpress	202
Snapchat	32
Shein	29

[893] Accounted period: 01/01/2025-30/05/2026.

[894] Accounted period: 01/01/2025-30/05/2026.

[895] Stripchat has been omitted from the list of VLOPs and VLOSEs by the European Commission in 2025 and is therefore not included in the table.

Regarding account terminations, the database records approximately 70 million permanent account removals. Instagram accounted for 97% of these terminations, followed by TikTok with 2%. These figures suggest notable differences in enforcement approaches across platforms, with some services relying more heavily on permanent account removal while others appear to favour temporary account restrictions. The services listed in the table below are those that reported scam-related account terminations in the DSA Transparency Database during the relevant period.

Table 11 - Scam-related account terminations[896]

Designated service[897]	SoRs (in thousands)
Instagram	68.141
TikTok	1.673
Facebook	321
Apple App Store	1
Pinterest	1

The table below presents the number of actions taken following notices received and the median time required to take action across the different designated services. The data are drawn from the most recent publicly available DSA Transparency reports[898] according to Article 16 DSA of the respective VLOPSEs.

Table 12 - Notices and takedowns

Designated services	Number of notices received	Number of actions taken (aggregated)	Median time to take action	Time unit[899]
AliExpress	28,932	3,390	8	hours
Amazon	10,577	1,628	28	days
App Store	211	N/A	92	days
Bing	N/A	N/A	N/A	N/A
Booking.com	382	7	501.65	not specified
Facebook	1,732	745	9.8	hours
Google[900]	22	N/A	43	not specified
LinkedIn	118	16	18	not specified
Instagram	95	61	18.32	hours
Pinterest	N/A	N/A	N/A	N/A

[896] Accounted period: 01/01/2025-30/05/2026.

[897] Stripchat has been omitted from the list of VLOPs and VLOSEs by the European Commission in 2025 and is therefore not included in the table.

[898] As of 30/05/2026.

[899] Unless stated, the time unit is not specified by the platforms.

[900] All Google services included.

Designated services	Number of notices received	Number of actions taken (aggregated)	Median time to take action	Time unit[899]
Pornhub	8,848	N/A	1.3	hours
Shein	443	0	N/A	N/A
Snapchat	896	450	4	days
Temu	3,708	N/A	16.58	not specified
TikTok	71,632	N/A	N/A	N/A
Zalando	0	0	N/A	N/A
Wikipedia	0	0	N/A	N/A
X	2,629	3	2	hours
XNXX	0	0	0	N/A
XVideos	171	171	14.66	not specified

Analysis

Removal and suspension mechanisms are widely used across platforms to restrict offenders and prevent their return. While some platforms maintain internal blocklists designed to prevent previously sanctioned actors from creating new accounts or advertising profiles, others may temporarily suspend accounts or delete pieces of scam-related content.[901] Nevertheless, third parties have raised **concerns regarding the responsiveness, transparency, and overall effectiveness of platform enforcement systems**.[902] One interviewee noted that when platforms fail to act, responsibility for filtering scams is shifted to external actors, such as telecommunications providers or cybersecurity companies.[903] As a result, enforcement efforts may become less efficient and more resource-intensive, requiring downstream actors to address harmful content and fraudulent activity that could have been prevented or disrupted earlier within the platform environment. At the same time, the effectiveness of automated enforcement must also be considered alongside the risk of over-moderation.[904] Detection systems that prioritise the rapid identification of scam-related content may generate false positives, potentially resulting in the removal or restriction of legitimate content.[905]

Despite the substantial volumes of content removals and account restrictions reported by platforms, some stakeholders have raised questions regarding **the speed and transparency of platforms' notice-handling procedures**.[906] Fact-checking

[901] Interview 14.

[902] Multi-stakeholder Workshop on Online Financial Scams.

[903] Interview 11.

[904] Council of Europe, Regulating content moderation on social media to safeguard freedom of expression (2025), available at: https://pace.coe.int/pdf/b11c97ecb434dedaec11f776b5c93c3dc5031b006e0be15e71c1e47227a78873/doc.%2016089.pdf.

[905] ibid.

[906] Multi-stakeholder Workshop on Online Financial Scams.

organisations within the EDMO network report significant delays before scam content is removed and, in some cases, an absence of meaningful feedback following reports submitted through platform reporting channels.[907] Similar concerns have been raised by BEUC regarding Google's designated services, with claims that Google would have taken more than six weeks to process reports, including those submitted by trusted flaggers.[908] An independent study of TikTok estimated an expected takedown delay of approximately 54 days for scam-related content.[909]

At the same time, evidence from trusted flagger organisations finds that platforms can remove scam content quickly and accurately under certain reporting arrangements, suggesting that enforcement outcomes depend not only on the evidence submitted but also on how platforms prioritise and process different categories of reports. Debunk.org submitted 1,468 reports through Meta's enforcement systems concerning 26,255 Facebook pages associated with fraudulent and illegal activity.[910] These submissions resulted in 1,465 successful enforcement actions, corresponding to a reported takedown rate of 99.8%.[911] Nevertheless, Debunk.org reports that response times averaged 75.4 hours in 2025, with individual reporting periods ranging from 7.4 to 332.8 hours.[912] FactReview similarly reported 49 successful notices concerning health and financial scams, with an average decision time of 2.65 days.[913] These findings suggest that the effectiveness of notice-and-action systems may depend not only on the quality of the evidence submitted but also on the reporting channel used and the resources available for review.

Beyond response times, third parties have questioned whether platforms consistently remove fraudulent content once it has been identified.[914] BEUC identified 503 advertisements believed to be scams on Facebook and Instagram, of which only 146 were removed, while more than 300 reportedly remained active.[915] In one example involving an advertiser operating under the name 'Fast Loan', four advertisements were reported for allegedly breaching EU consumer protection and consumer credit rules.

[907] European Digital Media Observatory (EDMO), Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU (2025), available at: https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.

[908] European Consumer Organisation (BEUC), Sponsored by Scammers: How Big Tech Platforms Facilitate Financial Fraud (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf.

[909] Bao Tran Truong et al., Audit of takedown delays across social media reveals failure to reduce exposure to illegal content (2026), available at: https://arxiv.org/html/2502.08841v3.

[910] Debunk.org, Debunk.org Trusted Flagger 2025 Report (2025), available at: https://www.debunk.org/debunk-org-trusted-flagger-2025-report.

[911] ibid.

[912] ibid.

[913] FactReview, Trusted Flagger Report #2 (2026), available at: https://factreview.gr/2026/03/03/trusted-flagger-report-2-en/.

[914] Multi-stakeholder Workshop on Online Financial Scams.

[915] European Consumer Organisation (BEUC), Sponsored by Scammers: How Big Tech Platforms Facilitate Financial Fraud (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf.

Meta removed one advertisement, two were removed by the advertiser itself, and one report received no response.[916] On TikTok, approximately 40% of notices submitted by BEUC members as part of the experiment were either rejected or resulted in no action in 2025.[917] Consumer groups also identified nine advertisements published by 'TRIPSOFT LIMITED' promoting 'fast cash' services; only one advertisement was removed, while the remaining reports were not upheld.[918] Similarly, on Google's designated services, three of the twenty advertiser accounts reported by BEUC members were ultimately removed.[919] One advertiser, 'FASTLOANADVANCE LLC', reportedly remained active despite promoting fast loans without credit checks and despite multiple reports submitted to the platform.[920]

These findings point to a broader challenge concerning enforcement escalation and repeat-offender management. For example, OIAT claims that platforms such as Facebook or Instagram may remove reported scam pages without proactively identifying related account variations or replacement pages.[921] CERT Polska similarly alleges that accounts responsible for disseminating malicious advertisements would rarely be blocked, enabling fraudsters to continue exploiting existing infrastructures with limited disruption.[922]

Additional concerns relate to the **ability of platforms to identify and track repeat offenders.**[923] OIAT claims that TikTok's advertising system would allow advertisers to conceal their identities through self-selected or automatically generated usernames.[924] Furthermore, both TikTok's and Google's advertising repositories have been described by OIAT as insufficiently transparent and difficult to analyse, because of, *inter alia*, missing targeting parameters.[925] Stakeholders have also reported that fraudulent advertisements can be reactivated under similar names after accounts are suspended, and that clearly fraudulent ads placed by the same advertiser are not always removed once an account is flagged, recommending that associated accounts be checked upon removal.[926] These limitations may also make it more difficult for researchers and regulators to assess whether enforcement actions are applied consistently across advertisers and campaigns.

---

[916] ibid.

[917] ibid; Consumer groups reported 360 ads on TikTok. 74 ads were rejected, and 73 ads were ignored (147 ads in total).

[918] ibid.

[919] ibid.

[920] ibid.

[921] ÖIAT, AdGuardians (2026), available at: https://research.oiat.at/adguardians.

[922] CERT Polska, Ad fraud on large online platforms (2024), available at: https://cert.pl/en/posts/2024/12/Ad-fraud-on-large-online-platforms/.

[923] Multi-stakeholder Workshop on Online Financial Scams.

[924] ÖIAT, AdGuardians (2026), available at: https://research.oiat.at/adguardians.

[925] ibid.

[926] Multi-stakeholder Workshop on Online Financial Scams.

Measure 4: Detection of coordinated scam networks

General overview

The detection of coordinated scam networks builds upon the countermeasures described above, including automated detection, human review, and removal mechanisms. While the latter focus primarily on identifying and enforcing against individual pieces of content, accounts, advertisements, or applications, the former seeks to **identify and disrupt the broader networks that enable scam operations to function**. It is therefore considered a distinct countermeasure because its objective extends beyond individual violations to the underlying systems, actors, and relationships that support fraudulent activity.

This additional layer of analysis is necessary because fraudulent intent is often difficult to establish from individual pieces of content alone. Content that appears legitimate on the surface may form part of a wider scam operation that only becomes apparent when associated websites, domains, accounts, applications, transactions, or other linked entities are examined.[927] By analysing these connections, platforms can attribute multiple activities to the same operation and identify patterns that would not be visible through content-level review alone. Given that online financial scams are frequently organised through interconnected networks of accounts, advertisements, websites, applications, and other services, addressing individual violations in isolation may have limited impact.[928] Platforms therefore increasingly seek to identify and disrupt the underlying infrastructure supporting scam operations through network analysis, behavioural signals, and cross-service intelligence.

This countermeasure is directly relevant to the risk factor of organised crime infrastructure and fraud-as-a-service models (Section 3.2.6), addressing the coordinated and networked character of many scam operations that span multiple accounts, campaigns, and platforms. The measure also addresses risks arising from account creation and verification (Section 3.1.1), insofar as network-level detection can identify replacement accounts and related entities that evade individual account-level enforcement. It is also partially relevant for risks associated with advertising systems by linking fraudulent advertisements to broader campaign infrastructures.

Information from designated services

Across the 2025 SRAs, a sizeable group of platforms reports no specific measures on the detection of coordinated scam networks (Apple App Store, Booking.com, Pornhub, Shein, Temu, Wikipedia, XNXX, Xvideos, and Zalando).

Among platforms that do report such processes, a common thread is the focus on identifying relationships and patterns across accounts, transactions, and behaviours. For example, Amazon states that it explicitly contrasts its newer knowledge-graph and deep graph neural network systems with traditional signal-by-signal detection, while Bing similarly reports combining web-scale graph analytics with human analysis to trace fraudulent infrastructure back to known threat actors.[929] Google reports using LLMs and

[927] Interview 12.

[928] Interviews 12, 13.

[929] Amazon, Bing 2025 Systemic Risk Assessment Reports.

behavioural detection on its designated services to surface interconnected networks of deceptive websites and ranking-manipulation schemes, and Facebook, Instagram, Pinterest, Snapchat, TikTok, and X all describe similar pattern-based systems for identifying coordinated spam, fake engagement, or linked advertiser and account activity.[930]

Uniquely, AliExpress reports an approach centred on recidivism, maintaining tracking databases to identify repeat offenders, account takeovers, and re-entry attempts by previously banned sellers rather than emphasising graph-based relationship discovery.[931]

Analysis

The scale and structure of online financial scams make infrastructure-level disruption increasingly necessary. In the context of scam advertisements, for example, individual advertisements often reach relatively few users, meaning that the removal of single advertisements may have limited impact on the overall operation.[932] **Scam campaigns typically rely on large volumes of content distributed across interconnected accounts, websites, domains, applications, and other services**. Consequently, analysing and dismantling the broader infrastructure behind a scam operation may often be more effective than focusing solely on individual manifestations of it.

A key aspect of this approach is examining the **destination and downstream infrastructure associated with suspicious content**. One interviewee noted that elements such as redirect chains, payment flows, domain registration patterns, hosting arrangements, and the reuse of website templates may provide stronger indicators of fraudulent activity than the visible content itself.[933] Content that initially appears legitimate may be revealed as fraudulent once associated landing pages and linked infrastructure are examined, enabling platforms and investigators to attribute multiple assets to the same underlying campaign.[934]

Infrastructure disruption encompasses a broad range of measures. These include account-level enforcement strategies that go beyond removing individual advertisements by suspending advertiser accounts or identifying and dismantling clusters of linked accounts operating as part of a coordinated scam network, often before additional fraudulent content is published. As noted by an interviewee, disruption efforts may also target technical infrastructure through domain takedowns, registrar and hosting-provider abuse reports, content delivery network abuse reports, URL blocking, certificate and

[930] Google, Facebook, Instagram, Pinterest, Snapchat, TikTok, and X 2025 Systemic Risk Assessment Reports.

[931] AliExpress 2025 Systemic Risk Assessment Report.

[932] Interview 11; Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll.

[933] Interview 13.

[934] Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll.

domain monitoring, and the provision of intelligence to law enforcement authorities for action against scam infrastructure.[935]

Given the volume of information involved, **automated systems play an important role in identifying connections between accounts, domains, advertisements, transactions, and other entities**. AI-based tools can assist in organising, prioritising, and correlating large datasets to identify which assets belong to the same campaign, enabling faster detection and disruption of scam networks.[936] However, these systems require careful calibration to minimise false positives and overly broad enforcement.[937] Human review therefore remains necessary to validate findings, while user reports provide an additional feedback mechanism that can help identify threats missed by automated systems and support continuous improvement.[938]

A study by AI Forensics developed methodologies for identifying coordinated political advertising campaigns by analysing semantic and behavioural similarities across advertisements, advertisers, and pages.[939] Rather than assessing individual advertisements in isolation, the methodology examined broader duplication patterns, including translated content, near-identical messaging, and reworded campaign materials. Drawing on techniques originally developed to identify coordinated information operations, the study found that behavioural and semantic relationships can reveal coordination between ostensibly independent actors.[940] Similar behavioural and semantic analyses could be used to identify coordinated fraudulent advertising campaigns, detect networks of related scam accounts operating under different identities, and reveal patterns of repeated or adapted scam content that may not be identifiable when advertisements are assessed individually.

At the same time, the detection and disruption of coordinated scam networks face important structural limitations. One interviewee reiterated that **scam operations frequently span multiple platforms, sectors, and jurisdictions, allowing fraudsters to exploit gaps between different organisations and regulatory frameworks**.[941] Several stakeholders interviewed as part of this study have therefore highlighted the potential value of structured information-sharing mechanisms between platforms and trusted cybersecurity providers.[942] Such mechanisms could enable the exchange of risk signals and threat intelligence without requiring broad access to platform data, potentially improving the ability to identify and disrupt scams before users are exposed.[943]

---

[935] Interview 14.

[936] Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll.

[937] Interview 14; Multi-stakeholder Workshop on Online Financial Scams.

[938] ibid.

[939] AI Forensics, No Embargo in Sight (2025), available at: https://aiforensics.org/uploads/No_Embargo_in_Sight_AI_Forensics_Report.pdf.

[940] ibid.

[941] Interview 12.

[942] Interviews 10, 11, 12, 14.

[943] ibid.

Despite the importance of infrastructure-level analysis, some stakeholders argue that platform enforcement systems continue to operate primarily at the level of individual content items rather than the broader networks behind them.[944] Gen claims that moderation systems frequently remove detected scam advertisements without escalating enforcement to the advertiser, campaign, or network level.[945] As a result, identical copies of fraudulent advertisements may continue circulating, sometimes from the same advertiser or from replacement accounts created specifically for that purpose. The organisation also reports that the widespread use of short-lived advertisements and disposable advertiser infrastructures further reduces the effectiveness of content-level enforcement, as the cost of replacing accounts remains low for organised scam operators.[946]

Related concerns have also been raised regarding **enforcement displacement**. Actions taken on one platform may result in migration rather than cessation, with fraudsters creating replacement accounts, moving to other services, or redirecting users towards external websites and messaging applications.[947] Investigations cited by EUobserver similarly suggested that scam advertisements detected on Facebook and Instagram were not always systematically linked to broader advertiser patterns or related campaigns.[948] These findings indicate that effective scam mitigation may require greater emphasis on identifying and disrupting the wider infrastructures that enable fraudulent activity rather than focusing exclusively on individual pieces of content.

Measure 5: Recommender system protection measures

General overview

Recommender system protection measures are crucial to prevent online financial scams from benefiting from algorithmic visibility and amplification. As recommendation, ranking, and discovery systems increasingly determine what content users encounter online, they have become important targets for scammers seeking to maximise reach and legitimacy.[949] Scam actors increasingly seek to exploit these channels because content surfaced through organic discovery mechanisms, including search rankings, recommendation systems, trending features, and autocomplete functions, may be perceived as more trustworthy and can attract users without relying on direct

[944] Multi-stakeholder Workshop on Online Financial Scams.

[945] Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-II.

[946] ibid.

[947] European Union Intellectual Property Office, Social Media – Discussion Paper: New and Existing Trends in Using Social Media for IP Infringement Activities and Good Practices to Address Them (2021), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Social_Media/2021_Social_Media_Discussion_Paper_FullR_en.pdf.

[948] EUobserver, Google's AI search feature raises concerns over scams and misinformation (2025), available at: https://euobserver.com/digital/aradc7eaf8.

[949] Interview 9.

advertising.[950] Online platforms, therefore, **play a critical role in shaping content discoverability through recommender systems as well as in preventing scammers from exploiting these systems.**

This countermeasure is directly relevant to the risk factor of recommender systems and algorithmic amplification (Section 3.1.1), which the report identifies as a primary mechanism through which scam content acquires visibility and perceived legitimacy. By integrating anti-scam safeguards into recommendation, ranking, and discovery systems, this measure directly mitigates risks arising from the algorithmic distribution of fraudulent content to targeted audiences.

Information from designated services

Based on the 2025 SRAs, nearly half the platforms (Apple App Store, Bing, Booking.com, LinkedIn, Pornhub, Shein, Temu, Wikipedia, XNXX, and XVideos) report no specific information on recommendation or ranking-based integrity measures.

Among the other platforms, a recurring approach is decoupling content moderation from recommendation eligibility, whereby content need not be removed outright to be suppressed from visibility. Instagram describes borderline or policy-adjacent content remaining available but allegedly ineligible for surfaces like Explore, Snapchat categorises manipulative 'engagement bait' as 'Not Eligible for Recommendation' without necessarily removing it, and Pinterest reports applying ranking-quality signals and eligibility criteria to reduce visibility of spam and low-quality content rather than deleting it.[951]

Several commerce-oriented platforms report linking recommendation suppression directly to trust or risk signals about the underlying seller or product: AliExpress ties its recommendation pool to Chief Risk Office controls and buyer-feedback signals, Amazon suppresses autocomplete and search results where queries suggest intent to find infringing products, and Zalando claims to prioritise reliable merchants while reducing visibility of problematic listings.[952]

Facebook, Google's designated services and X describe broader visibility-filtering and demotion mechanisms tied to integrity-based ranking signals.[953] Uniquely, TikTok describes virality-specific interventions, including manual review triggered at popularity thresholds and machine-learning 'dispersion techniques' intended to prevent repeated recommendation of similar harmful content, alongside user-facing controls to adjust recommendation exposure.[954]

---

[950] European Union Intellectual Property Office, Search Engines – Challenges and Good Practices to Limit Search Traffic Towards Intellectual Property Infringing Content and Services (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf

[951] Instagram, Snapchat, Pinterest 2025 Systemic Risk Assessment Reports.

[952] AliExpress, Amazon, Zalando 2025 Systemic Risk Assessment Reports.

[953] Facebook, Google, X 2025 Systemic Risk Assessment Reports.

[954] TikTok 2025 Systemic Risk Assessment Report.

Analysis

Recommender systems constitute a core distribution infrastructure for online scams. They are embedded within everyday content consumption pathways, including search, social feeds, and recommendation surfaces. Scam exposure therefore occurs through **algorithmically curated environments** that prioritise engagement, relevance, and personalisation, which can make fraudulent content harder to distinguish from legitimate content.[955]

Research published by The Hacker News highlights how this infrastructure can be systematically exploited.[956] Specifically, it describes an 'AI-driven pushpaganda' model in which scammers generate large quantities of AI-produced fake-news articles hosted on actor-controlled domains and specifically optimised for Google Discover recommendation signals, including topicality, engagement potential, and ranking relevance.[957] These operations exploit recommendation and search infrastructures to distribute deceptive content organically to profiled audiences.[958] Users are subsequently encouraged to activate browser push notifications, which are then used to deliver fake security alerts, fraudulent warnings, and scam redirects leading to additional malicious websites.[959] In this model, recommendation systems themselves become vectors for scam amplification, while SEO manipulation ensures that fraudulent pages are indexed, surfaced, and ranked in ways that increase their visibility and perceived legitimacy. These dynamics create a structural dependency on platform governance.

Scam operations are embedded in recommendation-driven user journeys, so effective countermeasures must target exposure and ranking. One interviewee claimed that platforms control recommendation systems and therefore determine the visibility and amplification of fraudulent content.[960] Third-party actors, including cybersecurity organisations and researchers, mainly contribute by identifying scam patterns and developing detection approaches, without the ability to intervene in distribution systems due to limited access to online platforms.[961] Within this context, **the EUIPO highlights measures such as demotion, de-indexing, ranking adjustments, and exclusion from recommendation eligibility as key tools** for limiting exposure to fraudulent content, particularly where immediate removal is not feasible.[962]

---

[955] Interview 3; Multi-stakeholder Workshop on Online Financial Scams; see also Gen, Gen Q4/2025 Threat Report (2026), available at: https://www.gendigital.com/blog/insights/reports/threat-report-q4-2025;.

[956] The Hacker News, AI-Driven Pushpaganda Scam Exploits Google Discover to Spread Scareware and Ad Fraud (2026), available at: https://thehackernews.com/2026/04/ai-driven-pushpaganda-scam-exploits.html.

[957] ibid.

[958] ibid.

[959] ibid.

[960] Interview 14.

[961] Interview 13.

[962] European Union Intellectual Property Office (EUIPO), Search Engines – Challenges and Good Practices to Limit Search Traffic Towards Intellectual Property Infringing Content and Services (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf.

5.3. User-facing protection measures

User-facing protection measures operate at the point of interaction between platform and end user, constituting a layer of countermeasures that complements upstream access controls and automated detection systems by equipping users themselves with tools and information to identify, report, and resist online financial scams. This category encompasses reporting mechanisms through which users, consumer organisations, public authorities, and trusted flaggers may notify platforms of suspected scam content; information about redress that guides victims through available post-scam steps; and friction tools intended to interrupt the urgency and impulsivity upon which scam operators rely. These measures intervene at the moment of user engagement, providing structured pathways for human-initiated identification and response that supplement platform-side enforcement.

Measure 1: Reporting tools

General overview

Reporting mechanisms are the main procedural route through which **users, consumer organisations, public authorities, and trusted flaggers may bring suspected scam content to the attention of VLOPs and VLOSEs**. Under the DSA, these mechanisms form part of the general notice-and-action framework for illegal content. Article 16 DSA requires hosting providers to maintain electronic mechanisms that are easy to access and user-friendly, and that allow any individual or entity to notify specific items of information that they consider to be illegal. Related provisions address statements of reasons (Art. 17 DSA), internal complaint handling (Art. 20 DSA), trusted flaggers (Art. 22 DSA), transparency reporting (Art. 24), and complaints to Digital Services Coordinators (Art. 53 DSA). In practice, these mechanisms can act as a countermeasure against online financial scams by providing a structured means for users, organisations, and public authorities to flag suspected fraudulent content for platform review and action, thereby supplementing automated detection with human-initiated identification across a broad range of content types and services.

Scam-related reporting may concern a range of online content and services, including advertisements, profiles, app listings, search results, marketplace listings, sponsored posts, direct links, and external landing pages. Depending on the platform and its interface, reports may be submitted through general illegal-content forms, terms-and-conditions reporting tools, advertising-specific channels, product-specific forms, or trusted-flagger pathways. Some platforms provide labelled scam or fraud categories, while others route scam-related reports through broader categories such as misleading content, illegal goods or services, impersonation, fraud, or other policy violations.

This countermeasure addresses risks arising from the operational complexity of scam schemes (Section 3.2) by providing users, consumer organisations, public authorities, and trusted flaggers with structured mechanisms to flag suspected fraudulent content. Reporting tools are broadly relevant across risk factors identified in Section 3.1.1, including advertising systems, account creation and verification, e-commerce integration, and profile discovery, as they enable human-initiated identification of fraudulent content across all platform surfaces.

Information from designated services

Several structural commonalities emerge regarding the reporting tools implemented. The large majority of VLOPs and VLOSEs – with the exception of Apple's AppStore, Facebook, Instagram, Google's designated services, and LinkedIn – do not offer a dedicated 'scam' or 'fraud' reporting category; instead, scam-related reports are channelled through a general-purpose mechanism covering all types of illegal content or policy violation. As a result, users may need to self-classify financial scam reports under generic headings with no tailored intake guidance.[963] Reporting tools are embedded at the level of individual content items through contextual menus or dedicated buttons placed close to the content.

Several platforms, such as AliExpress, Apple's App Store, Google's designated services, Facebook, Instagram, Snapchat, TikTok, and X, operate a dual-track architecture – one pathway for terms-and-conditions violations, another DSA-specific pathway for illegal content.[964] Multiple platforms, including Apple's AppStore, Facebook, Instagram, Pinterest, Snapchat, and Temu, emphasise that user-submitted notices are processed at least in part through human review.[965] This process is described above in Section 5.2. Most platforms describe appeal or redress mechanisms that reference the statement-of-reasons and complaint-handling frameworks of Articles 17 and 20 DSA, and several integrate Trusted Flagger pathways giving priority processing to notices from entities designated under Article 22 DSA.

Analysis

Article 16(1) DSA establishes the right of any individual or entity to notify hosting service providers of allegedly illegal content through a standardised notice-and-action mechanism that must be easy to access, user-friendly, and available exclusively by electronic means.[966] Article 16(2) specifies the minimum content of a valid notice: a sufficiently substantiated explanation of the alleged illegality, a precise electronic location of the content, the notifier's contact details, and a declaration of accuracy and completeness.[967] Where a notice is sufficiently clear to enable a diligent provider to identify the illegality without detailed legal examination, it may give rise to actual knowledge or awareness for the purposes of the liability regime established under Article 6 DSA (Article 16(3)).[968] Recital 50 further clarifies that reporting tools should be positioned in close proximity to the content in question to facilitate identification of the specific item reported.[969]

[963] Multi-stakeholder Workshop on Financial Scams.

[964] AliExpress, Apple AppStore, Google, Facebook, Instagram, Snapchat, TikTok, X 2025 Systemic Risk Assessment Reports.

[965] Apple AppStore, Facebook, Instagram, Pinterest, Snapchat, Temu 2025 Systemic Risk Assessment Reports.

[966] Digital Services Act, Article 16(1).

[967] ibid, Article 16(2).

[968] ibid, Articles 6 and 16(3).

[969] ibid, Recital 50.

The DSA Transparency Database, operational for VLOPs since 26 September 2023 and extended to all online platforms from 17 February 2024, is the primary publicly accessible repository for statements of reasons (SoRs) submitted following content moderation decisions. In the first 100 days, approximately 1.49 billion SoRs were submitted across 16 VLOPs.[970] These figures must be treated with caution as an indication of the functioning of the notice-and-action mechanism: SoRs arise from moderation decisions taken on any basis – including proactive automated detection and terms-of-service enforcement – not only responses to user-initiated notices.

The relationship between incoming Article 16 notices and outgoing SoRs is not transparent in publicly available data. A qualitative analysis of transparency reports from seven VLOPs in 2024 found that platforms did not specify the moderation action taken for a given category of Article 16 notice, leaving the process largely opaque.[971] Article 15(1)(b) DSA requires platforms to report the number of notices received and categorise them by action taken, but in practice granularity varies substantially.[972] A 2024 analysis indicates that Article 16 notices would be dominated by intellectual property infringements, hate speech, nudity, and violence, with financial scams not consistently appearing as a separate category.[973] Because most platforms channel scam reports through general illegal-content pathways without dedicated classification, scam-related notices are often invisible in the aggregate data. This is intensified by the absence of any harmonised taxonomy between the Transparency Database and platform reports prior to July 2025[974], with the first harmonised transparency reports not published until February 2026.[975]

The structural and operational shortcomings of the notice-and-action mechanism have been documented across institutional, academic, and civil-society sources, and they converge on a number of recurring themes.

First, **most platforms offer no dedicated scam or fraud reporting category**, requiring users to self-classify their notice under generic headings, and those operating a dual-track architecture (distinguishing terms-of-service violations from illegal content) offer no guidance for making that distinction. This is an aspect currently under investigation by the Commission in relation to Facebook and Instagram.[976] The Commission is also

[970] Amaury Trujillo et al., The DSA Transparency Database: Auditing Self-reported Moderation (2025), available at arxiv.org/abs/2312.10269.

[971] Alexander von Humboldt Institut fuer Internet und Gesellschaft, The DSA's Transparency Reports (2025), available at: https://www.hiig.de/en/analysis-of-the-dsas-transparency-reports/.

[972] Digital Services Act, Article 15(1)(b).

[973] Crowell & Moring, Notice and Action Mechanisms in the DSA (2024), available at: https://www.crowell.com/en/insights/client-alerts/notice-and-action-mechanisms-in-the-dsa-balancing-the-removal-of-illegal-content-and-the-freedom-of-expression.

[974] European Commission, How the Digital Services Act Enhances Transparency Online (2026), available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency

[975] ibid.

[976] European Commission, Commission Preliminarily Finds TikTok and Meta in Breach of Their Transparency Obligations Under the Digital Services Act (2025), available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503.

investigating whether users of these platforms can provide explanations or supporting evidence when contesting a moderation decision.[977]

BEUC claims that the reporting mechanisms on Facebook and Instagram require users to provide URLs yet consistently reject reports submitted with URLs, processing only those that include the ad's internal ID number, contrary to the platform's own instructions.[978] BEUC also claims that these platforms shift the burden of demonstrating illegality onto users, requiring them to identify the specific law breached and provide evidence and even case law, which BEUC considers to materially exceed the Article 16(2) standard.[979] Similarly, BEUC alleges that TikTok restricts users to 200 characters to justify a report, limiting their ability to substantiate their claims, and that Google's designated services initiate unnecessary 'conversations' requesting information already provided, adding friction and discouraging completion.[980]

To address this issue, stakeholders suggest that **platforms could redesign their notice-and-action mechanisms, providing accessible, clearly labelled pathways for reporting financial scam content and ensuring notices are processed with appropriate diligence**.[981] One interviewee has also highlighted that making reporting mechanisms more easily accessible to users increases the likelihood of users reporting suspicious activity, whereas complex reporting mechanisms reduce reporting rates.[982] To this end, it has been proposed by stakeholders that platforms introduce dedicated, clearly labelled scam and fraud reporting categories that guide users without forcing them into generic headings, together with review processes able to assess the contextual evidence scam reports typically require. Such categories could be accompanied by contextual prompts that collect the information needed to assess a report, rather than placing the burden on reporters to prove illegality.[983] Researchers consider that this approach would limit the risk of deterring victims from reporting, thus lowering the rate of under-reporting.[984]

Second, Article 17 DSA requires platforms to notify reporters of any decision taken, with a clear statement of reasons, legal or factual grounds, and available redress options.[985] According to the Humboldt Institute for Internet and Society's analysis of transparency reports, statements of reasons often amount to formulaic notifications providing limited

[977] ibid.

[978] BEUC, Sponsored by Scammers (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf.

[979] ibid.

[980] ibid.

[981] Multi-stakeholder Workshop on Financial Scams.

[982] Interview 11.

[983] Leijie Wang et al, From Inquisitorial to Adversarial: Using Legal Theory to Redesign Reporting Systems in Online Communities (2026), available at https://arxiv.org/pdf/2506.07041.

[984] Eiman A. Al-Hamad et al, Reporting Social Media Fraud: Motivations, Barriers, and Reporting Mechanism in Mahmoud Barhamgi et al (eds) Web Information Systems Engineering (2024), available at https://doi.org/10.1007/978-981-96-0570-5_29.

[985] Digital Services Act, Article 17.

information.[986] For financial scam reports, where moderation outcomes may carry significant financial and personal consequences, this inadequacy may be especially acute: reporters may not be able to reliably tell whether their contextual evidence was considered, whether a human reviewer was involved, or what evidentiary threshold was applied.

The investigation published by BEUC illustrates this concern. In BEUC's opinion, Facebook's and Instagram's responses were vague and never clearly explained; the platforms even suggested users 'reach out to the party responsible for posting the content to resolve your issue with them directly'.[987] BEUC holds that the statements of reasons relied exclusively on preformulated wording, such as a generic reference to paragraph 3.2 of the Terms of Service, without specifying which legal provision had been breached.[988] The consumer organisation also claims that TikTok did not motivate its rejections, generally claiming 'insufficient evidence' even for clearly fraudulent ads.[989] In one case document by BEUC, Google cited 'defamation' as the ground of its decision, despite this aspect not being raised or concerned by the report.[990] Facebook, Instagram and TikTok were also found by BEUC to handle near-identical ads inconsistently: the organisation documented cases where identical legal argumentation on ads with substantially identical wording produced different outcomes: one was removed and the other not.[991] The organisation also claims TikTok applied different practices across Member States, removing an ad in one country while leaving it active in others despite uniform EU rules.[992]

The third structural concern is the **asymmetry between individual users and Trusted Flaggers** designated under Article 22 DSA.[993] That provision allows Digital Services Coordinators to award Trusted Flagger status to entities with particular expertise in detecting illegal content, provided they are independent of platforms and submit notices diligently, and requires platforms to prioritise their notices and process them without undue delay. Researchers claim that organisations with the institutional capacity to obtain this designation have materially better prospects of timely review than individual users.[994]

BEUC provided empirical evidence of this difference: on Meta, almost all ads reported by trusted flaggers were taken down, whereas individual and organisational reports were

[986] Alexander von Humboldt Institut fuer Internet und Gesellschaft, The DSA's Transparency Reports (2025), available at hiig.de/en/analysis-of-the-dsas-transparency-reports/.

[987] BEUC, Sponsored by Scammers (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf.

[988] ibid.

[989] ibid.

[990] ibid.

[991] ibid.

[992] ibid.

[993] Digital Services Act, Article 22.

[994] Jacob van de Kerkhof, Article 22 Digital Services Act: Building Trust with Trusted Flaggers (2025), available at: https://policyreview.info/pdf/policyreview-2025-1-1828.pdf.

frequently rejected or ignored, a pattern EDMO also corroborates.[995] BEUC also holds that on TikTok trusted flaggers received acknowledgements and decision notifications that were not extended to other reporters.[996] The German consumer organisation vzbv corroborates this: of 60 ads reported across 13 platforms, only 28 were removed, suggesting that effectiveness depends heavily on the notifier's institutional standing.[997] Similarly, Greece Fact Check reports that the content moderation decisions on Facebook depended on the type of user who submitted the notice.[998] The organisation claims that where regular users flagged content as fraudulent, the platform did not take any measures, finding that the post did not violate its rules; however, where the same content was reported by Greece Fact Check, as a trusted flagger, the posts were removed.[999]

Designation as a trusted flagger does not, however, guarantee positive processing. ÖIAT reports that Facebook and Instagram did not remove or block any of the fake webshop pages it flagged on their services between late April and mid-May 2025[1000] and EDMO has relayed similar concerns on behalf of other fact-checking organisations.[1001] Stakeholders note that trusted flaggers face further obstacles, including being temporarily blocked for reviewing too many scam sites, disparities in reporting effort across platforms, the absence of case identifiers, and instances in which fewer than 1% of submissions were not actioned.[1002]

Against this background, the empirical evidence on platform responses to financial scam reports is instructive. Between December 2025 and March 2026, BEUC and 13 consumer organisations across 13 Member States identified and reported approximately 893 financial scam advertisements on Facebook, Instagram, TikTok, and Google's designated services. Only 27% of notices resulted in removal, while 52% were rejected

[995] BEUC, Sponsored by Scammers (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf; EDMO, Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU (2025), available at: https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.

[996] BEUC, Sponsored by Scammers (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf.

[997] vzbv, Bericht zur Tätigkeit als Trusted Flagger (2026), available at: https://www.vzbv.de/en/trusted-flagger-reports-illegal-content-are-not-being-adequately-processed-platforms-0.

[998] EDMO, Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU (2025), available at: https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.

[999] EDMO, Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU (2025), available at: https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/.

[1000] ÖIAT, Numerous fraudulent ghost stores on Facebook and Instagram (2025), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Ghost_Stores_Erhebung_en.pdf.

[1001] ibid.

[1002] Multi-stakeholder Workshop on Online Financial Scams.

or received no response.[1003] The platform-level breakdown reveals significant variation: Facebook and Instagram rejected 43% of 503 notices and ignored a further 18%, removing only 29%; TikTok removed only 22% of 360 reported ads, while claiming in 37% of cases that the ad had been removed by the advertiser before review; Google removed 60% of 30 reported ads but rejected or ignored the remainder.[1004] This data, despite focusing only on a subset of designated services (Facebook, Instagram, Google's designated services and TikTok) under a limited geographical scope (13 Member States), is the most comprehensive empirical assessment of notice and action mechanisms in the financial scam context publicly available at the time of writing.[1005] Its findings inform the picture of the functioning of reporting mechanisms, and are complemented by the civil-society documentation cited above from EDMO, vzbv and ÖIAT.[1006]

Stakeholders also claim that platforms appear to under-remove or delay action on financial scam content relative to other categories of illegal material. The Humboldt Institute for Internet and Society's analysis of VLOPs' transparency reports across the first two reporting cycles of 2024 indicates that moderation activity was concentrated in categories such as hate speech, nudity, violence, and spam.[1007] To that end, the Reuters investigation previously cited in this report alleges that the perceived lack of focus on financial scam content would result from the substantial advertising revenue earned by platforms from fraudulent ads.[1008]

Victim under-reporting further compounds the limitations of the notice-and-action mechanism. The Financial Action Task Force (FATF) has observed that cyber-enabled scams are likely under-reported, especially where losses are negligible, and that emotional factors such as embarrassment and fear frequently deter victims from coming forward.[1009] Research on pig-butchering scams found that 26.9% of participants said fear of judgment stopped them from reporting to authorities, while 69.2% found the associated terminology offensive and dehumanising, further reducing reporting.[1010] The scam reports actually submitted through reporting mechanisms therefore represent only a fraction of the fraudulent content users encounter, rendering the currently reported removal rates incomplete.

[1003] BEUC, Sponsored by Scammers (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf.

[1004] ibid, p. 12.

[1005] ibid.

[1006] ibid.

[1007] Alexander von Humboldt Institut fur Internet und Gesellschaft, The DSA's Transparency Reports (2025), available at http://hiig.de/en/analysis-of-the-dsas-transparency-reports/.

[1008] Reuters, Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show (2025), available at: https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

[1009] FATF, Egmont Group and INTERPOL, Illicit Financial Flows from Cyber-Enabled Fraud (2023), available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html.

[1010] Rajvardhan Oak and Zubair Shafiq, Lifecycle and Impact of Pig-Butchering Scams (2025), available at: https://arxiv.org/abs/2503.20821.

Measure 2: Information on redress

General overview

For victims of online financial scams, information about redress can **indicate the steps available after a suspected scam, including routes for reporting, account security, payment-related action, and contact with public authorities**. Scam victims often may need to preserve evidence, notify payment providers, report offending accounts or advertisements, and identify the competent public authority or platform channel. Information presented through platform help pages, public authority portals, or dedicated scam resources can describe these steps and distinguish platform reporting from external complaint, law enforcement, or payment channels. Information about redress forms part of the user-facing information environment surrounding platform decisions and user reports, while remaining distinct from the substantive operation of redress mechanisms themselves.

This countermeasure is primarily relevant to victim-level vulnerability factors (Section 3.3), addressing the information asymmetry that victims face after scam exposure. By providing structured guidance on reporting pathways, payment recovery, account security, and contact with public authorities, information on redress may lower the psychological and practical barriers that prevent victims from taking appropriate post-scam action. The measure does not directly address upstream risk factors identified in Section 3.1.1. However, by improving the victim experience and potentially increasing reporting rates, the measure may indirectly support detection and enforcement measures that rely on user-submitted reports.

Information from designated services

The majority of platforms do not describe any dedicated scam redress mechanisms, scam information centres, or specific victim support services in their DSA risk assessment reports. Where redress-adjacent measures do exist, they overwhelmingly take the form of general-purpose consumer protection mechanisms – such as refund guarantees, customer service complaint channels, and notice-and-action reporting tools – rather than scam-specific resources.

Among the platforms examined, only Facebook's and Instagram's risk assessment reports refer to providing users with information on relevant external support channels, such as law enforcement authorities, consumer protection bodies, or financial institutions, following a financial scam.[1011]

Facebook and Instagram are also the only platforms that describe dedicated scam-focused user-facing resources: Meta's Scam Protection Centre provides guidance specifically about financial scams across both platforms.[1012] Meta's Help Center directs users who encounter suspected scams on Facebook Marketplace to stop communicating and report the relevant seller, buyer, or listing, while its phishing guidance refers users

[1011] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[1012] Meta, Scam Protection Center, available at: https://www.meta.com/safety/scam-protection-center/?srsltid=AfmBOorv_e8hnzHjxUpa0AzmtGH3gl4LaLs4jyV-D8CmTB0Uc8Gp4bcz.

to account-recovery and account-security resources.[1013] In addition, the centre offers users the possibility of being redirected to local support services. However, this functionality is not available across all countries and, at the time of writing, was limited to five EU Member States (Denmark, France, Italy, Poland, Romania).[1014]

Snapchat provides a Safety Resources and Support page with country-specific information – however, the information provided does not generally refer to scam redress, only covering financial sextortion risks.[1015] Snapchat reports that it has actively supported the external StopThinkFraud anti-fraud campaign.[1016] TikTok references scams as a topic covered in its Safety Centre resources, though without elaborating on their content.[1017]

Among e-commerce platforms, the pattern diverges towards financial remediation rather than informational support. Amazon's A-to-Z Guarantee, AliExpress's refund and return policies, and Temu's Purchase Protection Program all offer concrete financial redress (refunds) that may apply to scam situations, though none are framed as scam-specific tools.[1018] Booking.com uniquely describes actively working with affected travellers to find alternative accommodation when illegal listings are identified.[1019]

Analysis

As illustrated in the preceding section, the vast majority of VLOPs and VLOSEs do not, in their DSA risk assessment reports, describe providing users with any specific information on who to contact externally following a financial scam encounter. The question is what added value a platform-facing redress measure would deliver to victims if adopted voluntarily, and whether regulators, consumer advocates, and existing practice support it.

The DSA itself imposes no such duty. The notice-and-action mechanism under Article 16 provides a right for any individual to notify a platform of illegal content,[1020] and although the European Commission has emphasised that this mechanism extends to online shopping scams and financial fraud, the Commission's own guidance acknowledges that notice-and-action 'is not part of a possible scam recovery process'

[1013] Meta, Scam Protection Centre, available at: https://www.meta.com/en-gb/safety/scam-protection-center/?srsltid=AfmBOorTxDhBz-GGBuTgOt2PPUwtLQ8ANvrpBwiQStKyV-uw9gHCy8wn.

[1014] Meta, Local Support, available at: https://www.meta.com/en-gb/safety/scam-protection-center/safety-tips/local-support/.

[1015] Snap, What you need to know about Financial Sextortion, available at: https://values.snap.com/safety/financial-sextortion.

[1016] Snapchat, 2025 Systemic Risk Assessment Report.

[1017] TikTok 2025 Systemic Risk Assessment Report.

[1018] Amazon, AliExpress, Temu 2025 Systemic Risk Assessment Reports.

[1019] Booking.com, 2025 Systemic Risk Assessment Report.

[1020] Digital Services Act, Article 16(1).

and does not direct victims to appropriate external bodies.[1021] The internal complaint-handling provisions under Articles 20 and 21 likewise address content moderation decisions, not victim support.[1022]

The principal benefit of a voluntary measure therefore lies in reducing the fragmentation of the external redress landscape that a victim must otherwise navigate alone. Redress-relevant information is dispersed across national law enforcement and fraud-reporting portals, the European Consumer Centres Network (ECC-Net), financial supervisory channels, and, ultimately, the courts, with no single authoritative gateway consolidating victim-specific guidance on the sequence of steps – contacting one's bank, reporting to the platform, notifying the Digital Services Coordinator (DSC), approaching national police cybercrime units, or consulting ECC-Net – that a victim ought to follow, and no EU-level scam information centre**. A platform that surfaced this information at the moment of the scam encounter would spare victims from assembling it themselves, often under conditions of significant distress and urgency**. A model to that end is the United Kingdom's Report Fraud hub, which provides guidance on protection against scams and allows users to file reports.[1023]

The uneven state of existing channels underscores the point. Europol directs citizens to national reporting portals but acknowledges that these vary from country to country, with some Member States offering no dedicated online option and leaving victims to attend a police station in person.[1024] France operates the PHAROS platform for reporting illicit online content, the Netherlands hosts a centralised internet-fraud reporting facility, and Germany's DSC, the Bundesnetzagentur, provides consumer guidance that advertises out-of-court dispute settlement bodies and certified trusted flaggers.[1025]

At EU level, ECC-Net assisted over 125,000 consumers in 2023 and intermediated directly with traders to obtain redress in approximately 22,500 cases, operating through 150 legal experts in 24 languages.[1026] For victims of platform-facilitated financial scams, however, its mandate is of limited use: ECC-Net expressly excludes disputes involving fraudulent activity on the part of the trader and transactions in financial and investment products such as gambling, investment funds, cryptocurrencies, and stock markets, which are among the categories of scams commonly encountered on designated services.[1027] Moreover, ECC-Net lacks any power to compel traders, relying on

[1021] European Commission, Fighting Online Scams with DSA (2025), available at https://digital-strategy.ec.europa.eu/en/policies/dsa-notice-and-action-mechanism.

[1022] Digital Services Act, Articles 20 and 21.

[1023] UK Report Fraud, available at: https://www.reportfraud.police.uk/.

[1024] Europol, Report Cybercrime Online, available at: https://www.europol.europa.eu/report-a-crime/report-cybercrime-online (noting that in Member States without a dedicated online reporting option, victims must go to a local police station).

[1025] Bundesnetzagentur, Bundesnetzagentur helps make online shopping safer (2025), available at https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2025/20251128_DSC.html.

[1026] ECC-Net, High Demand for ECC-Net's Services: 9 Million Euro Recovery for Consumers, available at: https://www.eccnet.eu/news/high-demand-ecc-nets-services-9-million-euro-recovery-consumers.

[1027] ECC-Net, Our Services, available at: https://www.eccnet.eu/ecc-network/our-services, explicitly listing among cases where ECC-Net is unable to assist: those involving fraudulent activities on the part of the trader; and those concerning financial and investment products including gambling, investment funds, cryptocurrencies, and stock markets.

persuasion and cooperation; this renders its involvement largely ineffective against the organised, malicious operations documented in this report.[1028]

Authoritative bodies increasingly locate responsibility for protecting scam victims with the platforms themselves, though they stop short of prescribing a concrete signposting standard, and dedicated literature specifically endorsing platform-surfaced redress information remains limited. Victim Support Europe recommends that scam victims report to their regional fraud centre, a European Consumer Centre, a cybersecurity centre, and the police.[1029] The practical value of that advice, however, depends on victims independently identifying the relevant bodies in their jurisdiction and navigating each one's prerequisites and exclusions – exactly the burden a platform is positioned to relieve. The European Commission's guidance on fighting online scams advises victims to 'contact your bank first to ask for a chargeback, secure your accounts, and report to local authorities,' but this appears only on the Commission's own digital-strategy website, with no mechanism requiring platforms to surface equivalent information to affected users.[1030]

Germany's Bundesnetzagentur actively advertises out-of-court dispute settlement bodies and trusted flaggers to consumers, showing that signposting redress is regarded as valuable within the DSA architecture. The fact that the substance of the advice victims need is already articulated by regulators and advocates, yet confined to institutional websites victims may never reach, is a strong argument for platforms relaying it at the point of harm. One interviewee also noted that, beyond platform reporting mechanisms, victims face a fragmented reporting landscape involving multiple actors, including banks, law enforcement authorities, and telecom providers.[1031]

Practice outside the EU shows that centralised, user-facing redress information is workable. Australia's Scams Prevention Framework designates the digital-platforms sector as a regulated sector overseen by the Australian Competition and Consumer Commission and requires regulated entities, including platforms, to maintain internal and external dispute-resolution pathways for scam complaints on a 'no wrong door' basis, so that a victim may raise a complaint with any entity connected to the scam.[1032] Singapore's ScamShield ecosystem offers a single public-facing resource: a 24/7 helpline (1799) that users can call to check suspected scams, obtain advice, and, where they have been victimised, be directed to participating banks, with guidance that distinguishes between flagging suspicious indicators through the app and filing an official police report where money has been lost.[1033]

[1028] ibid; European Disability Forum, Enforcement Toolkit: European Consumer Centres Network, available at: https://www.edf-feph.org/enforcement-toolkit-european-consumer-centres-network/, noting that ECCs have no enforcement powers and cannot force traders to comply with the law.

[1029] Victim Support Europe, Fraud – Victim Support Europe, available at https://victim-support.eu/help-for-victims/info-on-specific-types-of-victims/fraud-victims/.

[1030] European Commission, Fighting Online Scams with DSA (2026), available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-notice-and-action-mechanism.

[1031] Interview 13.

[1032] Lexology, The new Scams Prevention Framework: key considerations for regulated entities (2025), available at https://www.lexology.com/library/detail.aspx?g=416897c5-ef22-4ea2-8d67-17758aac87b2.

[1033] Singapore Government, ScamShield, available at: https://www.scamshield.gov.sg/

Measure 3: Friction tools

General overview

Friction tools – **deliberate design interventions that introduce pauses, warnings, or confirmation steps to slow harmful or impulsive user behaviou**r – represent a theoretically well-supported but practically underdeveloped response to financial scam content on VLOPs and VLOSEs. The scam victimisation literature consistently identifies urgency, authority impersonation, and social proof as the mechanisms by which scammers suppress deliberative reasoning, and friction is designed to interrupt precisely this dynamic at the point of engagement. Stakeholders have also recommended embedding friction tools into platform and payment interfaces to counteract the urgency and impulsivity on which many scams rely.[1034] Yet the current landscape is one of fragmentation and absence.

This stands in marked contrast to the payment sector, where friction mechanisms are increasingly mandatory and have demonstrated measurable impact. Confirmation-of-payee checks verify that the recipient's name matches the account before a payment is authorised, flagging impersonation and misdirection to the payer; cooling-off periods temporarily hold first-time, high-value, or otherwise high-risk transfers so the customer can be asked targeted questions and reconsider before irrevocable funds leave the account; and dynamic scam warnings replace generic notices with real-time, in-app alerts calibrated to the specific risk profile of the transaction.

This countermeasure is directly relevant to the psychological manipulation techniques deployed by scammers (Section 3.2.3), which exploit urgency, authority impersonation, and social proof to suppress deliberative reasoning. Friction tools are designed to interrupt these dynamics at the point of user engagement, creating pauses, warnings, or confirmation steps that restore the opportunity for critical evaluation. The measure partially addresses risks associated with direct messaging functions and e-commerce integration (Section 3.1.1), where scammers seek to move users rapidly toward financial commitment.

Information from designated services

A significant proportion of the platforms reviewed – including Amazon, Apple App Store, Booking.com, Pinterest, Shein, Wikipedia, XVideos, and Zalando – do not report any friction tools specifically designed to prevent or mitigate fraudulent or scam-related interactions. Where friction tools are reported, they tend to fall into a few recurring categories: warnings triggered when users attempt to navigate away from the platform or interact with external links, content interstitials or labels that provide contextual information before users engage with sensitive or unverified content, and protective measures aimed specifically at minors, such as warnings when teens begin conversations with strangers.

Meta's March 2026 announcement described the rollout of real-time pop-up warnings on Facebook about suspicious friend requests, flagging risk indicators such as recently created accounts, unusual geographic location, and absence of mutual connections; warnings for potentially fraudulent device-linking attempts on WhatsApp; and an expanded Messenger feature that analyses chat behaviour patterns for signs of

[1034] Multi-stakeholder Workshop on Online Financial Scams.

manipulation and warns users before they are defrauded.[1035] The announcement was notably silent on new user-facing friction protections for Instagram.

Several divergences in scope and focus can be observed. LinkedIn reports a large number of friction tools, including warnings when conversations are moved off-platform, safety reminders for European members, message filtering with dismissible warnings, and blurred sensitive content.[1036] Facebook and Instagram report the largest number of friction tools overall, though these are spread across several content categories – including hate speech, state-controlled media, and minor safety – rather than being concentrated on scams specifically.[1037] TikTok reports similar content warnings.[1038] Temu is the only e-commerce platform reviewed that reports counterfeit-specific search alerts guiding at the point of user search.[1039] The adult content platforms (Pornhub, XNXX) report friction mechanisms focused on age verification and content deterrence rather than scam prevention.[1040]

In general, none of the designated services reviewed that offer financial transaction functions report friction tools in the form of transaction-level confirmation steps, payment delays, or verification prompts before completing purchases.

Analysis

The concept of friction, as a deliberate design choice, draws on nudge theory and choice architecture: small, non-coercive interventions that shape behaviour without excluding options.[1041] 'Protective friction' includes deliberate interruptions designed to slow harmful or impulsive behaviour.[1042] In the EU legislative context, Article 25 DSA encodes this distinction negatively: it prohibits platforms from designing interfaces that 'deceive or manipulate' users or 'otherwise materially distort or impair' their ability to make free and informed decisions, with Recital 67 explicitly naming such practices as 'dark patterns.'[1043]

[1035] Meta, Fighting Scammers and Protecting People With New Technology and Partnerships (2026), available at: https://about.fb.com/news/2026/03/fighting-scammers-protecting-people-with-new-technology-and-partnerships/.

[1036] LinkedIn 2025 Systemic Risk Assessment Report.

[1037] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[1038] TikTok, Integrity and Authenticity, available at: https://www.tiktok.com/safety/en/policies-and-engagement/integrity-authenticity.

[1039] Temu 2025 Systemic Risk Assessment Report.

[1040] Pornhub, XNXX 2025 Systemic Risk Assessment Reports.

[1041] Richard H. Thaler and Cass R. Sunstein, Nudge: Improving Decisions About Health, Wealth and Happiness (2008), available at: https://www.researchgate.net/file.PostFileLoader.html?id=53abe564cf57d7df1e8b45f4&assetKey=AS%3A273548994646025%401442230571326.

[1042] Cass R. Sunstein, Sludge and Ordeals (2019), available at https://scholarship.law.duke.edu/dlj/vol68/iss8/6/; see also the conceptual overview in Newall, What Is Sludge? Comparing Sunstein's Definition to Others (2023) available at https://research-information.bris.ac.uk/ws/portalfiles/portal/321458464/Review_of_sludge_Newall.pdf.

[1043] Digital Services Act, Article 25(1) and Recital 67 DSA.

The DSA's prohibition of user-hostile design therefore defines the space in which protective friction is the corresponding affirmative instrument.

Financial scam content is a particularly apt context for friction deployment. The scam victimisation literature consistently identifies urgency, authority impersonation, and social proof as the principal mechanisms scammers use to suppress deliberate reasoning and elicit fast, unreflective compliance.[1044] Research applying dual-process theory to telecom network fraud finds that scammers deliberately construct high-pressure, ambiguous scenarios to activate fast information processing while undermining slower, analytical evaluation.[1045] The theoretical logic of friction is to interrupt this process at the point of engagement – inserting a pause, confirmation prompt, or warning before the user proceeds.

The inverse dynamic is observable online: an OIAT study of Meta's advertising ecosystem found that fraudulent ads and their linked landing pages systematically employ manipulative design patterns that are the functional opposite of protective friction – including artificial scarcity (‘Only 2 items left’), manufactured urgency (‘Today only’), confirmshaming (framing inaction as personal failure), and interface interference (prominent call-to-action buttons alongside barely visible exit options or links to terms and conditions).[1046] These deceptive design elements form a central component of the narratives used by fraudulent advertisers to induce consumers into fast, unreflective action – precisely the behavioural dynamic that protective friction is designed to counteract.[1047] One Stakeholder emphasised that **as scam journeys often span multiple platforms, it is important to provide warnings at each transition point rather than only at the initial point of contact**.[1048] They also noted that early-stage warning messages can effectively disrupt the sense of urgency exploited by scammers, but that current platform terms of service often prevent third parties from displaying such warnings within platform environments, limiting the scalability of this approach.[1049]

No large-scale empirical study has evaluated friction interventions specifically in the context of financial scam advertising on VLOPs or VLOSEs. Some stakeholders have, however, stated that **friction pages which interrupt user actions are more effective in scam prevention than awareness efforts**.[1050] Timing is also essential: warnings have to be placed before any payment details or credentials are shared.[1051] The evidence

[1044] See Fuming Xu et al., 'Victimization Mechanisms and Countermeasures in Telecom Network Fraud: A Dual-System Theoretical Perspective' (2025), available at https://www.frontiersin.org/journals/psychology/articles/10.3389/fpsyg.2025.1637935/full; Feedzai and Global Anti-Scam Alliance, 2023 State of Scams Report (2024), available at https://gasa.org/knowledge-base/reports/global-state-of-scams-report-2023.

[1045] ibid.

[1046] Österreichisches Institut für angewandte Telekommunikation, Analyse des Betrugsökosystems Online-Werbung auf Meta-Plattformen (2025), available at: https://www.rtr.at/medien/aktuelles/publikationen/Publikationen/Publikationen_2026/Betrugso-kosystem_Werbung_KommAustria_final.pdf.

[1047] ibid.

[1048] Interview 14.

[1049] Interview 14.

[1050] Interviews 3, 11.

[1051] Interview 14.

base is drawn from adjacent contexts, principally misinformation sharing, phishing prevention, and browser security warnings, and its generalisability to the financial scam context should be treated with care.

Browser security warnings provide the most directly comparable data point to scam-adjacent platform interventions. Active, interaction-requiring interstitial warnings were found to protect users from malware and phishing sites in approximately 75–90% of cases across a field study of 25 million warning impressions, a significant improvement on passive contextual labels.[1052] However, warnings that produced many false positives showed substantially higher override rates. Chrome's SSL certificate warning, for example, recorded a click-through (override) rate of 70.2%; this pattern was interpreted as indicative of 'warning fatigue.'[1053]

Subsequent research demonstrates that this fatigue is a measurable, neurobiological phenomenon; for example, it was established that habituation – a 'decreased response to repeated stimulation' – develops in the brain over time and produces a substantial decline in warning adherence as exposure accumulates.[1054] Taken together, these findings reinforce the caveat for deploying warnings at scale: **any friction tool encountered repeatedly across millions of daily interactions risks progressive loss of effectiveness regardless of its initial design quality, unless it is deliberately engineered against habituation.**

Friction tools have existing precedents in financial contexts. Confirmation of Payee (CoP), deployed in the UK and Australia, verifies whether a payee's account name matches the recipient details entered before a transfer completes, prompting the payer where a mismatch is detected.[1055] With the entry into force of the Instant Payment Regulation, this has also been introduced in the EU.[1056] Some banking applications deploy in-app warnings flagging potentially fraudulent payment requests; research indicates that even minor changes to such notifications can substantially reduce authorised push payment (APP) fraud, with the largest effects from combining risk-based and call-to-action warnings over time.[1057] At the platform level, the UK Payment Systems Regulator's mandatory APP-scam reimbursement regime and the EU's forthcoming PSD3 and Payment Services Regulation have prompted providers toward stronger

[1052] Devdatta Akhawe and Adrienne Porter Felt, Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness (2013), available at: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe; Serge Egelman, Lorrie Faith Cranor and Jason Hong, You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings (2008), available at: https://doi.org/10.1145/1357054.1357219.

[1053] ibid.

[1054] Anthony Vanceet al., Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments (2018), available at: https://www.jstor.org/stable/26630238.

[1055] Deloitte, Forecasting the Rise of Push Payment Scams (2024), available at https://www.deloitte.com/us/en/insights/industry/financial-services/authorized-push-payment-fraud.html.

[1056] Regulation (EU) 2024/886 of the European Parliament and of the Council of 13 March 2024 amending Regulations (EU) No 260/2012 and (EU) 2021/1230 and Directives 98/26/EC and (EU) 2015/2366 as regards instant credit transfers in euro (Text with EEA relevance), OJ L, 2024/886.

[1057] TrueLayer, What Is Authorised Push Payment (APP) Fraud? (2024), available at https://truelayer.com/blog/payments/what-is-authorised-push-payment-fraud/.

friction measures.[1058] The strongest effectiveness data currently derive from browser-security and banking contexts rather than social-media scam interfaces.

The broader picture is one of fragmentation: where friction tools exist, they typically address the moment of communication or navigation rather than the point of financial commitment. This stands in marked contrast to the payment sector, where friction tools are considerably more developed and, in some jurisdictions, mandatory. Thirteen of 28 jurisdictions assessed in a global review of anti-scam measures have incorporated compulsory payment frictions such as warnings, holds, and confirmation-of-payee mechanisms.[1059] No platform reviewed reports independent evaluation of the effectiveness of its friction tools, and none discloses data on user override rates, the proportion of interactions in which warnings were displayed relative to the volume of scam content present, or the behavioural impact of specific warning formats.

5.4. Structural level governance and policies

Structural-level governance and policies encompass the foundational rules and institutional frameworks through which platforms define, prevent, and address online financial scams. As a systemic layer of risk governance, they shape all downstream detection, moderation, and enforcement activities. Rather than targeting individual content or conduct, these measures establish the conditions under which platform ecosystems operate, including prohibited conduct definitions, disclosure requirements, eligibility criteria, verification obligations, and rules governing the restriction or removal of content, advertisements, products, or accounts. This category includes platform governance policies, enforcement frameworks, and cross-sector cooperation mechanisms integrating intelligence from financial institutions, signal-sharing infrastructures, and trusted flagger networks. Together, these measures embed preventive safeguards into platform design, onboarding, advertising, and business verification processes, while extending detection beyond individual platforms to enable the early identification of coordinated fraudulent activity through the collective analysis of signals from multiple sources.

Measure 1: Platform-level policies

General overview

Platform governance policies constitute an important layer of platform risk governance. They establish the rules that determine which forms of content, behaviour, commercial activity, and service use are permitted, thereby **shaping how scams are defined, prevented, and addressed within platform ecosystems**. These policies underpin downstream detection, moderation, and enforcement systems by setting prohibited conduct, disclosure requirements, eligibility criteria, verification obligations, and the conditions under which content, advertisements, products, or accounts may be restricted

[1058] UK Payment Systems Regulator, APP Fraud Reimbursement Protections (2024), available at: https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/.

[1059] Consumers International, Stopping Online Scams: Building Consistency and Coordination for Consumers (2026) available at: https://www.consumersinternational.org/media/699948/consumers-international-stopping-online-scams-building-consistency-and-coordination-for-consumers.pdf, p. 20.

or removed. This could be a relevant countermeasure against online financial scams in that it establishes the framework within which fraudulent content and conduct are identified, prohibited, and sanctioned, while also embedding preventive safeguards into platform design, onboarding, and advertising processes that reduce the opportunity for scam operations to take hold.

Under the DSA, platforms are required to set out clear terms and conditions governing the use of their services (DSA, Article 14). The practical implementation of these rules, however, varies considerably across platforms. Some rely on structured enforcement frameworks, including graduated sanctions such as 'three-strikes' systems, while others apply more flexible or context-dependent approaches.[1060] More broadly, platform governance frameworks are increasingly extending beyond reactive moderation towards preventive measures embedded in platform design, onboarding processes, business verification systems, advertising controls, recommendation systems, and the development and deployment of AI-enabled products and services.[1061]

This countermeasure establishes the foundational governance layer that shapes all downstream detection, moderation, and enforcement activities. Platform-level policies are broadly relevant across all risk factors identified in Section 3.1.1, insofar as they define prohibited conduct, verification requirements, eligibility criteria, and enforcement conditions that determine how risks associated with advertising systems, account creation, recommender systems, direct messaging, e-commerce integration, and profile discovery are addressed.

Information from designated services

Across the 2025 SRAs, a common structural pattern is the layering of a general conduct or community policy with domain-specific rules targeting abuse vectors. For example, Meta combines its Community Standards and Advertising Standards with a dedicated Manipulated Media Policy and Coordinated Inauthentic Behaviour policy applicable across its designated services (Facebook and Instagram), X supplements its general Rules with a Platform Manipulation and Spam Policy and a Synthetic and Manipulated Media Policy, and TikTok and Snapchat both pair general Community Guidelines with distinct policies governing synthetic and AI-generated media.[1062]

E-commerce and marketplace platforms (AliExpress, Amazon, Google Shopping, Shein, Temu, and Zalando) converge on a similar policy architecture centred on seller/merchant conduct rules, product authenticity and counterfeit-goods provisions, and review-integrity requirements, with several going further to formalise rights-holder participation.[1063]

A generative-AI-specific governance layer is emerging but not yet universal: Bing's Image Creator Terms of Use, Snapchat's AI-specific Acceptable Use Policies, and

[1060] Interview 14.

[1061] European Union Intellectual Property Office (EUIPO), Apps and App Stores – Challenges and Good Practices to Prevent the Use of Apps and App Stores for IP Infringement Activities (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Apps_and_App_stores/2024_Apps_and_App_stores_FullR_en.pdf; Interview 12.

[1062] Facebook, Instagram, X, TikTok, Snapchat 20225 Systemic Risk Assessment Reports.

[1063] AliExpress, Amazon, Google, Shein, Temu, and Zalando 2025 Systemic Risk Assessment Reports.

TikTok's synthetic-media disclosure requirements each impose obligations on AI-generated content specifically.[1064]

Adult-content platforms (Pornhub, XNXX, Xvideos) again form a distinct cluster, with governance emphasis placed on uploader verification, content legality, and ownership obligations, reflecting the different risk profile of their content ecosystems.[1065]

Analysis

Although the designated services claim to have developed extensive policies addressing scams, third parties report discrepancies between formal rules and actual moderation outcomes.[1066] **Perpetrators of online scams quickly adapt their methods in response to new preventive measures, requiring platforms to continuously update both their policies and enforcement practices in a cyclical and responsive approach**.[1067]

Some stakeholders claimed that enforcement decisions do not always align with the platforms' own policy definitions; according to AI Forensics, among undeclared ads that are moderated as political, 60% were found not to fall into Meta's platform definitions.[1068] Conversely, fewer than half of the advertisements voluntarily declared as political by advertisers appeared to satisfy the platform's own criteria.[1069] Although arising in the context of political advertising, these findings suggest inconsistent classification of content under platform policies, which could undermine the effectiveness and predictability of platform scam countermeasures.

Another study by AI Forensics found that health-related advertisements that remained on platforms displayed practices expressly prohibited under platform advertising policies, including clickbait strategies, misleading medical claims, celebrity impersonation, and deceptive URLs that redirected users to fraudulent landing pages.[1070] The study also identified the systematic exploitation of platform features such as beneficiary and payer fields, display links that mask destination URLs, and page-name impersonation.[1071] These features enable advertisers to conceal their identities and evade enforcement mechanisms, allowing policy-violating advertisements to continue circulating even after individual advertisements are removed.[1072]

[1064] Bing, Snapchat, TikTok 2025 Systemic Risk Assessment Reports.

[1065] Pornhub, XNXX, Xvideos 2025 Systemic Risk Assessment Reports.

[1066] Multi-stakeholder Workshop on Online Financial Scams.

[1067] Interview 10; Multi-stakeholder Workshop on Online Financial Scams.

[1068] AI Forensics, No Embargo in Sight (2025), available at: https://aiforensics.org/uploads/No_Embargo_in_Sight_AI_Forensics_Report.pdf.

[1069] ibid.

[1070] AI Forensics, Meta's Failing Ad Moderation: Health Scams Targeting EU Users (2025), available at: https://aiforensics.org/work/meta-health-ads.

[1071] ibid.

[1072] ibid.

These findings may create uncertainty regarding the practical meaning of platform rules and complicate compliance efforts by advertisers and other users. More broadly, they raise questions about whether increasingly detailed policy frameworks can be applied consistently across large-scale moderation systems. Even where content is correctly identified as problematic, enforcement is not always extended to duplicate advertisements, coordinated campaigns, or related actors, limiting the scalability and effectiveness of policy implementation.[1073]

The governance arrangements across platform ecosystems may also be complex. In app-store environments, responsibility for user-generated content is often contractually assigned to app developers, creating layered accountability between the platform, the developer, and the end user.[1074] Similarly, governance within advertising ecosystems may be distributed across publishers, advertising intermediaries, merchants, and advertisers, each subject to different contractual terms and compliance obligations.[1075] Large product ecosystems such as Google and Amazon may simultaneously operate as publishers, marketplaces, and advertising intermediaries, and therefore maintain multiple sets of terms governing different activities and risk vectors. This can make the allocation of responsibilities for scam prevention and enforcement more complex in practice.

Measure 2: Cooperation with third parties

General overview

Cooperation between platforms and third-party actors has become a core component of scam detection and disruption, reflecting the **growing recognition that no single platform can fully identify scam patterns operating across financial, technical, and organisational ecosystems**.[1076] In practice, these measures can act as a countermeasure against online financial scams by pooling complementary intelligence across institutional boundaries, allowing platforms to surface coordinated fraudulent activity at an earlier stage and to respond more effectively to threats that operate across multiple services and sectors. Rather than relying solely on internal moderation systems, platforms increasingly integrate external intelligence flows from financial institutions, cross-industry signal-sharing infrastructures, and specialised trusted flagger networks. These systems are designed to extend detection beyond platform boundaries, allowing early identification of scam infrastructures that may only become visible when observed across multiple datasets and institutional perspectives.[1077] Cross-sector information sharing is presented as a key good practice because many harmful activities become

[1073] Multi-stakeholder Workshop on Online Financial Scams.

[1074] Interview 14.

[1075] ibid.

[1076] Interview 10; Multi-stakeholder Workshop on Online Financial Scams.

[1077] European Union Intellectual Property Office (EUIPO), Social Media – Discussion Paper: New and Existing Trends in Using Social Media for IP Infringement Activities and Good Practices to Address Them (2021), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Social_Media/2021_Social_Media_Discussion_Paper_FullR_en.pdf.

identifiable only when signals from multiple actors are combined.[1078] Individual indicators that appear benign in isolation may reveal coordinated abuse when analysed collectively.[1079]

This countermeasure addresses the cross-platform, cross-sectoral, and cross-jurisdictional character of organised scam operations (Section 3.2.6), recognising that effective scam mitigation requires intelligence pooling across institutional boundaries. Cooperation with third parties is directly relevant to risk factors that extend beyond individual platform control, including organised crime infrastructure and fraud-as-a-service models. The measure is also relevant for risks arising from account creation and verification, advertising systems, and e-commerce integration by enabling early identification of coordinated fraudulent activity through shared intelligence from financial institutions, cybersecurity organisations, and trusted flagger networks.

Information from designated services

Across the 2025 SRAs, third-party cooperation clusters around a few recurring partner types. A substantial subset of platforms (Apple App Store, Booking.com, LinkedIn, Pornhub, and Shein) report no specific information at all.

Intellectual-property rights holders form the most consistently cited cooperation category among marketplace platforms: AliExpress, Amazon, Temu, and Zalando all describe implementing dedicated channels through which rights holders report counterfeit or infringing listings.[1080]

Collaboration with external researchers and academia is another prominent theme among the platforms: Google's designated services, Facebook, Instagram, TikTok and X reference work with external researchers and industry stakeholders on manipulation and coordinated activity.[1081] Law-enforcement cooperation is explicitly named by a narrower group of platforms, including Facebook, Instagram, XNXX and Xvideos.[1082]

Industry-wide standards participation appears more selectively, with references to the Coalition for Content Provenance and Authenticity (C2PA) identified across the SRAs from Google's designated services, Amazon, Facebook, Instagram, Bing, LinkedIn and TikTok.[1083]

[1078] Interview 14; Multi-stakeholder Workshop on Online Financial Scams.

[1079] Interview 10; Multi-stakeholder Workshop on Online Financial Scams; see also European Union Intellectual Property Office (EUIPO), Search Engines – Challenges and Good Practices to Limit Search Traffic Towards Intellectual Property Infringing Content and Services (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf.

[1080] AliExpress, Amazon, Temu, and Zalando 2025 Systemic Risk Assessment Reports.

[1081] Google, Facebook, Instagram, TikTok, X 2025 Systemic Risk Assessment Reports.

[1082] Facebook, Instagram, XNXX and Xvideos 2025 Systemic Risk Assessment Reports.

[1083] Google, Amazon, Facebook, Instagram, Bing, LinkedIn and TikTok 2025 Systemic Risk Assessment Reports.

Analysis

There is broad consensus among stakeholders consulted as part of this study that combating online scams requires cooperation across multiple services, sectors, and jurisdictions, involving online platforms, financial institutions, telecommunications providers, cybersecurity actors, consumer-protection organisations, civil-society organisations, and law-enforcement authorities.[1084] Responsibility for tackling scams should not rest solely with online platforms but should be distributed across all actors capable of detecting, preventing, or responding to fraudulent activity through shared intelligence, coordinated interventions, and the disruption of criminal infrastructures.

A central component of this cooperation is **the exchange of intelligence between platforms and stakeholders**. Examples include the Global Signal Exchange, which facilitates the sharing of information on abusive websites, scam typologies, and threat indicators between technology companies, regulators, and other stakeholders.[1085] The initiative reportedly contains more than one billion signals contributed by over one hundred participating organisations.[1086] Similar approaches have emerged through sector-specific initiatives, such as the Fraud Intelligence Reciprocal Exchange (FIRE), which uses intelligence from financial institutions to identify scam operations and generate enforcement signals.[1087] Banking and telecommunications networks also provide reporting channels that feed intelligence into platform enforcement systems and wider anti-fraud ecosystems.[1088] Beyond data exchange between platforms and stakeholders, stakeholders interviewed as part of this study reported that data sharing between platforms themselves is also crucial to effectively combat scams.[1089] They also emphasised **the importance of closer collaboration with financial institutions to enable a more holistic response to online scams,** noting that digital policy and financial sector regulation often remain siloed, which can hinder coordinated and effective action across the scam ecosystem, warranting harmonisation.[1090]

Beyond information sharing, cooperation increasingly focuses on the **coordinated disruption of scam infrastructures**. Industry initiatives such as the Tech Against Scams Coalition (TASC), the Global Anti-Scam Alliance (GASA), and the Industry Accord Against Scams and Fraud launched at the UN Global Fraud Summit seek to facilitate cooperation between platforms, financial institutions, telecommunications providers, governments, and consumer-protection organisations.[1091] Complementing

[1084] Interviews 10, 11, 12, 13, 14; Multi-stakeholder Workshop on Online Financial Scams.

[1085] Interview 12; Multi-stakeholder Workshop on Online Financial Scams; see also Meta, Scams Are Bad for Business: Our Ongoing Efforts to Fight Fraud (2025), available at: https://about.fb.com/news/2025/12/scams-are-bad-for-business-metas-efforts-to-fight-fraud/.

[1086] Interview 12.

[1087] This initiative is led by Meta and is only active in the United Kingdom and Australia.

[1088] Meta, Scams Are Bad for Business: Our Ongoing Efforts to Fight Fraud (2025), available at: https://about.fb.com/news/2025/12/scams-are-bad-for-business-metas-efforts-to-fight-fraud/.

[1089] Interviews 11, 13, 15.

[1090] ibid.

[1091] Interviews 10, 12, 15; see also https://about.fb.com/news/2025/05/avoiding-investment-payment-scams-online/Meta, Avoiding Investment and Payment Scams Online (2025), available at: https://about.fb.com/news/2025/05/avoiding-investment-payment-scams-online/; Meta, Scams Are

these initiatives, the International Chamber of Commerce (ICC) and GASA have jointly published a Best Practices Framework for Combating Scam Advertising, providing practical guidance for advertisers, advertising intermediaries, digital platforms, and regulators on preventing, detecting, and responding to scam advertising through coordinated governance, information sharing, and transparent enforcement.[1092] These initiatives combine intelligence-sharing mechanisms with prevention activities, awareness campaigns, consumer-protection measures, and coordinated responses to emerging scam threats. Similar objectives underpin operational cooperation within the EMPACT framework, where law-enforcement authorities and service providers collaborate to prevent and disrupt online fraud through dedicated working groups and coordinated actions.[1093]

Cooperation also takes place through **structured reporting and escalation mechanisms**. Trusted flagger systems, specialised reporting channels, and dedicated fraud-reporting pipelines enable external organisations to submit high-quality reports and intelligence directly into platform enforcement processes. Examples include the DSA Trusted Flagger mechanism, Meta's Trusted Partner Programme, Google's Priority Flagger Programme, and reporting arrangements involving financial institutions and civil-society organisations.[1094] These mechanisms are intended to improve the speed and accuracy of detection by incorporating expertise and intelligence originating outside the platform itself.

At the same time, stakeholders identify several challenges to effective cooperation. Some interviewees described cooperation as uneven and, in certain cases, largely symbolic.[1095] While platforms frequently express willingness to collaborate with civil-society organisations, some partnerships are perceived by the interviewed stakeholders as focusing primarily on awareness-raising and public-facing initiatives rather than operational cooperation.[1096] Similar concerns have been raised by an interviewee regarding trusted flagger arrangements, which may shift part of the burden of detection and reporting onto external organisations without necessarily strengthening platforms' own detection capabilities.[1097] For instance, under the 'Permissions and Restrictions' section, YouTube's terms of service reportedly prohibit third parties from modifying what is displayed to users.[1098] As a result, according to stakeholders interviewed as part of

Bad for Business: Our Ongoing Efforts to Fight Fraud (2025), available at: https://about.fb.com/news/2025/12/scams-are-bad-for-business-metas-efforts-to-fight-fraud/.

[1092] GASA, ICC and GASA publish best practices framework for combating scam advertising (2026), available at: https://gasa.org/knowledge-base/blog/icc-and-gasa-publish-best-practices-framework-for-combating-scam-advertising.

[1093] Europol, EMPACT (2026), available at: https://www.europol.europa.eu/how-we-work/empact.

[1094] European Commission, Trusted Flaggers under the Digital Services Act (DSA) (2026), available at: https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa; Meta, Measuring Performance, available at: https://transparency.meta.com/governance/tracking-impact/measuring-performance/; Google, Partner Programs, available at: https://transparency.google/intl/en_mt/tools-programs/partner-programs/.

[1095] Interviews 13, 14.

[1096] ibid; Interview 11.

[1097] Interview 11.

[1098] YouTube, Terms of References (n.d.), available at: https://www.youtube.com/t/terms?hl=en&override_hl=1

this study, cybersecurity providers may be unable to warn users directly about advertisements they have identified as fraudulent.[1099]

More broadly, researchers and civil-society organisations report that **restrictions relating to APIs, incomplete datasets, limited access to ad libraries and content repositories, and the absence of systematic data-sharing mechanisms can hinder independent analysis and cooperation with third parties**.[1100] In addition, interviewees highlighted significant differences in platform responsiveness.[1101] While some platforms appear willing to engage and cooperate, others are perceived by these interviewees as unresponsive.[1102] These stakeholders also noted that certain platforms may prioritise confidentiality and reputational considerations, which can limit transparency.[1103] At the same time, they also expressed the concern that platforms may use collaboration with civil society for publicity purposes.[1104]

One interviewee proposed **the establishment of trusted intermediary structures capable of facilitating cooperation between private and public actors**.[1105] Europol was cited as a positive example, particularly because of its ability to receive, validate, and disseminate threat intelligence to national authorities through secure information-sharing arrangements such as the Traffic Light Protocol.[1106] Similar mechanisms were reported valuable for supporting trusted, scalable, and auditable cooperation between platforms, cybersecurity organisations, financial institutions, telecommunications providers, and public authorities.[1107] In this context, the forthcoming EU Action Plan against Online Fraud was reported as a potential vehicle for strengthening cooperation and establishing more structured channels for intelligence exchange and coordinated responses across the anti-scam ecosystem.[1108]

Stakeholders have also emphasised that effective online enforcement is not possible without offline enforcement, including international treaties across jurisdictions, and noted that some scams are facilitated at the state level by hostile actors.[1109]

[1099] Interview 13.

[1100] Interview 11; Multi-stakeholder Workshop on Online Financial Scams.

[1101] Interviews 11, 13.

[1102] ibid.

[1103] ibid.

[1104] ibid.

[1105] Interview 13.

[1106] ibid.

[1107] ibid.

[1108] ibid; European Commission, 2030 Consumer Agenda and Action Plan for Consumers in the Single Market – A New Impulse for Consumer Protection, Competitiveness and Sustainable Growth (2025), available at: https://commission.europa.eu/document/download/84cfc60e-f264-4f31-9f79-9ec83dce064d_en?filename=JUST_template_comingsoon_standard_14.pdf.

[1109] Multi-stakeholder Workshop on Online Financial Scams.

6. Case studies

The following section describes the findings of the four in-depth case studies carried out by the study team. The topics of the case studies have been selected in consultation with DG CONNECT to allow for an even deeper understanding of the operation of specific financial scams on different types of designated services, and of the platforms' responses.

6.1. Case study A: Finfluencers and online coaching on video-sharing platforms

Purpose of the case study

The proliferation of financial influencers and online financial coaching represents a complex dissemination environment for online investment scams. In recent years, finfluencer content and online investment coaching schemes on video-sharing platforms, where creators attract followers by displaying wealth and promising to share the knowledge required to replicate it, constitute a rapidly growing scam vector, particularly among younger demographics. Unlike traditional investment scams, harmful conduct may arise through a mixture of legitimate financial education, misleading promotion, undisclosed commercial interests, and, in some cases, outright scams. Finfluencers may knowingly promote fraudulent schemes, unknowingly amplify scams, or simply provide poor-quality financial advice that nevertheless causes consumer harm or redirects them to fraudulent content.

Scope and methodology

This case study prioritises video-sharing platforms hosting and amplifying finfluencer and online investment coaching content. It examines how platform design shapes exposure to finfluencer-related investment scams. The case study considers the designated services Facebook and Instagram (Meta), Snapchat, TikTok, YouTube and X as part of the scope.

Methodologically, the case study triangulates (i) DSA materials, including VLOP/VLOSE risk assessment reports, enforcement actions and the DSA Transparency Database data; (ii) regulatory alerts and enforcement by national consumer/product-safety authorities; (iii) academic literature and investigative reporting on finfluencers; (iv) targeted interview data from Tasks 1 and 2; (v) stakeholder input shared through the workshop (Task 4).

Background on scam model, prevalence and impact

Social media platforms have fundamentally transformed how financial information is produced, disseminated, and consumed. Online video-sharing platforms such as YouTube, TikTok, Instagram, Facebook, Snapchat and X have evolved into large-scale information ecosystems where entertainment, education, and commercial activity increasingly converge. Within these environments, influencers have emerged as important intermediaries capable of shaping consumer attitudes and user behaviours across a range of domains.[1110] A subset of these influencers are so-called 'finfluencers',

[1110] Antara Sen, Influence of Social Media and Finfluencers on Investor Behaviour (2026), available at: https://www.ijfmr.com/papers/2026/1/66685.pdf.

who are social media content creators disseminating information, commentary, recommendations, and educational material relating to personal finance, investing, and financial products.[1111] Their activities span a broad spectrum, ranging from basic financial literacy content and budgeting advice to the promotion of highly speculative investments, including cryptocurrencies, NFTs, forex trading products, algorithmic trading systems, and online business opportunities.[1112] While some finfluencers possess relevant professional qualifications, others operate outside traditional regulatory frameworks and may provide investment-related guidance without formal authorisation, supervision, or professional accountability.[1113]

The scam model commonly associated with finfluencers is based on aspirational marketing and authority-building. Followers are encouraged to believe that similar outcomes can be achieved by adopting the strategies, products, or services promoted by the content creator.[1114] The pathways through which scams may arise vary considerably. In some cases, finfluencers may knowingly engage in fraudulent activity by promoting fraudulent investment opportunities, financial products, or platforms.[1115] In other cases, they may unknowingly disseminate fraudulent financial content, for example, by promoting products or services without conducting adequate due diligence.[1116] A further pathway arises where finfluencer content serves as a gateway to other scammers, fraudulent websites, or investment scams operating elsewhere in the online ecosystem.[1117] Finally, some finfluencer accounts may themselves be fraudulent.[1118] These profiles may impersonate employees of established financial institutions, fund managers, or financial advisers, or falsely claim affiliations with

[1111] Essam Ghadafi and Panagiotis Andriotis (2025), UK Finfluencers: Exploring Content, Reach and Responsibility, available at: https://arxiv.org/pdf/2505.01941.

[1112] Henning Zülch, Marius Mölders and Christian Pieter Hoffmann, Navigating the rise of finfluencers: a multidimensional quality framework for strategic partnerships (2025), available at: https://www.econstor.eu/bitstream/10419/338848/1/41264_2025_Article_334.pdf; José M. Tomasena, Diego Arredondo and Hibai López-González (2025), Networking and monetization strategies of Spanish-speaking finfluencers: a co-link analysis of YouTube descriptions, available at: https://spir.aoir.org/ojs/index.php/spir/article/view/15343.

[1113] Antara Sen, Influence of Social Media and Finfluencers on Investor Behaviour (2026), available at: https://www.ijfmr.com/papers/2026/1/66685.pdf; ABBL, Finfluencers and generation Z: between financial education and risky advice (2026), available at: https://www.abbl.lu/finfluencers-and-generation-z-between-financial-education-and-risky-advice/.

[1114] Henning Zülch, Marius Mölders and Christian Pieter Hoffmann, Navigating the rise of finfluencers: a multidimensional quality framework for strategic partnerships (2025), available at: https://www.econstor.eu/bitstream/10419/338848/1/41264_2025_Article_334.pdf.

[1115] European Securities and Markets Authority (ESMA), Warning on Social Media and Investment Recommendations (2024), available at: https://www.esma.europa.eu/sites/default/files/2024-02/ESMA74-1103241886-912_Warnings_on_Social_Media_and_Investment_Recommendations.pdf.

[1116] Marius Mölders, Lennart Bock, Eloy Barrantes, and Henning Zülch, Understanding Finfluencers: Roles and Strategic Partnerships in Retail Investor Engagement (2025), available at: https://www.sciencedirect.com/science/article/pii/S0148296325002851.

[1117] ABBL, Finfluencers and generation Z: between financial education and risky advice (2026), available at: https://www.abbl.lu/finfluencers-and-generation-z-between-financial-education-and-risky-advice/; Antara Sen, Influence of Social Media and Finfluencers on Investor Behaviour (2026), available at: https://www.ijfmr.com/papers/2026/1/66685.pdf.

[1118] Finans Danmark, Styrket bekæmpelse af digital svindel - Svindel Task Forcens 18 anbefalinger (2024), available at: https://www.ft.dk/samling/20241/almdel/ERU/bilag/81/2948819/index.htm.

regulated firms and may direct followers to fraudulent investment platforms or employ other deceptive techniques designed to make unregistered or fictitious firms appear legitimate.[1119]

The primary victims of finfluencer-related investment scams are individuals who use social media and video-sharing platforms as sources of financial information and investment guidance. Traditional sources of financial advice increasingly compete with social media platforms that offer more accessible, personalised, and entertaining content formats, underlined by the peer-to-peer appearance of finfluencer content.[1120] Evidence suggests that reliance on social media for investment-related information is widespread. In Germany, more than half of investors aged 18-45 had received financial information from finfluencers in 2024, and approximately half of those had subsequently invested in the products being promoted.[1121] In the United Kingdom (UK), more than one in four individuals reported using social media, community messaging applications, or online forums for investment guidance in 2024. Among those relying on social media for investment advice, one in five cited free access to financial experts as a key motivation. The same study found that more than half of UK adults who use social media for investment guidance do not verify the reliability of finfluencers or the information they provide.[1122] Younger consumers appear to be particularly exposed to these risks. For many Millennials and members of Generation Z, social media has become a primary source of financial information and investment-related advice.[1123] A survey of 1,026 students in France and Belgium found that 46% sought financial information through social media, including 41.3% on TikTok and 13.6% on Instagram.[1124] In the United Kingdom, 44% of Generation Z respondents reported using information obtained through social media when making investment decisions in 2023.[1125] Similarly, in Germany, more than half of Generation Z and Millennial respondents viewed social media as an alternative to traditional sources of financial advice.[1126]

[1119] International Organization of Securities Commissions (IOSCO), Finfluencers (2025), available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD795.pdf; Federal Financial Supervisory Authority (BaFin), Guidance Notice on Investment Advice (2025), available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_250210_anlageberatung.html?nn=19659504.

[1120] Antara Sen, Influence of Social Media and Finfluencers on Investor Behaviour (2026), available at: https://www.ijfmr.com/papers/2026/1/66685.pdf.

[1121] Federal Financial Supervisory Authority (BaFin), Guidance Notice on Investment Advice (2025), available at: https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Merkblatt/mb_250210_anlageberatung.html?nn=19659504.

[1122] Barclays, Finfluencers: The Rise and Risks of Investment Content Creators (2024), available at: https://home.barclays/insights/2024/10/finfluencers-the-rise-and-risks-of-investment-content-creators/.

[1123] Antara Sen, Influence of Social Media and Finfluencers on Investor Behaviour (2026), available at: https://www.ijfmr.com/papers/2026/1/66685.pdf.

[1124] ABBL, Finfluencers and generation Z: between financial education and risky advice (2026), available at: https://www.abbl.lu/finfluencers-and-generation-z-between-financial-education-and-risky-advice/.

[1125] CFA Institute and FINRA Investor Education Foundation, Gen Z and Investing: Social Media, Crypto, FOMO, and Family (2023), available at: https://www.cfainstitute.org/about/press-room/2023/finra-cfa-institute-gen-z-research.

[1126] Federal Financial Supervisory Authority (BaFin), Finfluencer: Between Information and Investment Advice (2024), available at:

The actors involved in finfluencer-related investment scams may include both finfluencers themselves as well as broader networks of individuals or organised crime organisations. In some cases, finfluencers may be the primary perpetrators, deliberately promoting fraudulent investment opportunities, fictitious financial products, or scam platforms.[1127] In other cases, they may unknowingly disseminate misleading information, act as intermediaries for fraudulent actors, or encourage users to engage with products and services that subsequently expose them to financial scams.[1128] The boundaries between intentional deception, negligent promotion, and indirect facilitation are therefore often difficult to distinguish. These challenges are compounded by the low barriers to entry associated with becoming a finfluencer.[1129] As a result, a wide range of actors with differing levels of knowledge, intent, and accountability may participate in the dissemination of the scam. This diversity of actors makes it difficult to identify the ultimate offender, attribute responsibility, and determine whether the scam resulted deliberately or not.[1130]

Irrespective of whether a finfluencer is the direct perpetrator or otherwise involved in the dissemination of misleading content, the resulting harm to victims is broadly similar. The most immediate impact is financial loss arising from participation in fraudulent investment schemes or high-risk cryptocurrency-related products. Beyond financial losses, victims may also experience wider psychological and social consequences, including stress, anxiety, loss of trust in financial institutions or online information sources, and, in some cases, deterioration of personal relationships or changes in financial behaviour following the loss event (see Section 4.3 for detailed analysis). Victims may also be subject to recovery scams, as described in Section 4.3.2.[1131]

Relevance to EU citizens and regulatory priorities

Depending on the specific circumstances, finfluencer conduct may fall within the scope of several EU legal and regulatory frameworks.[1132] Where content constitutes a commercial communication promoting products or services, it may be subject to the Unfair Commercial Practices Directive, including its rules on misleading commercial practices and transparency of commercial intent. Where a finfluencer provides

https://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Fachartikel/2024/fa_bj_2409_Finfluencer.html?nn=161510.

[1127] European Securities and Markets Authority (ESMA), Warning on Social Media and Investment Recommendations (2024), available at: https://www.esma.europa.eu/sites/default/files/2024-02/ESMA74-1103241886-912_Warnings_on_Social_Media_and_Investment_Recommendations.pdf.

[1128] Marius Mölders, Lennart Bock, Eloy Barrantes, and Henning Zülch, Understanding Finfluencers: Roles and Strategic Partnerships in Retail Investor Engagement (2025), available at: https://www.sciencedirect.com/science/article/pii/S0148296325002851.

[1129] ibid.https://www.sciencedirect.com/science/article/pii/S0148296325002851?via%3Dihub

[1130] Henning Zülch, Marius Mölders and Christian Pieter Hoffmann, Navigating the rise of finfluencers: a multidimensional quality framework for strategic partnerships (2025), available at: https://www.econstor.eu/bitstream/10419/338848/1/41264_2025_Article_334.pdf.

[1131] Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545.

[1132] Felix Pflücke, Europe's Fragmented Approach to Finfluencer Regulation: Post #4 for the Blogposium on Finfluencers (2026), available at: https://corporatelawacademic.wordpress.com/2026/01/30/europes-fragmented-approach-to-finfluencer-regulation-post-4-for-the-blogposium-on-finfluencers/.

investment advice or investment recommendations relating to financial instruments, the activity may instead fall within the regulatory framework established by MiFID II and, where relevant, the Market Abuse Regulation. Similarly, recommendations concerning crypto-assets may trigger obligations under the Markets in Crypto-Assets Regulation (MiCA). Relevant national legislation may also apply depending on the nature of the activity and the competent supervisory authority. A key challenge lies in the qualification of finfluencer activity itself. In practice, it is often difficult to determine whether content constitutes investment advice, investment recommendations, commercial communication, or general commentary. As a result, a significant proportion of finfluencer activity may fall outside clearly defined supervisory categories, creating regulatory uncertainty regarding applicable obligations and enforcement thresholds.[1133]

In response to the rise of finfluencers in recent years, in 2024, the European Securities and Markets Authority (ESMA) issued a warning in 2024 for people posting investment recommendations on social media.[1134] Further, in 2026, the European Parliament called for the development of EU-wide standards to address misleading financial promotion, hidden advertising, and scams promoted by finfluencers.[1135]

Description of platform features relevant to scam propagation

Finfluencer-related investment scams exploit a combination of platform features with the objective of maximising user engagement, content visibility, and monetisation. According to researchers, content distribution systems on video-sharing platforms rely heavily on engagement-driven recommendation algorithms that prioritise material generating high watch time, interaction, and retention, resulting in finfluencer content being surfaced within personalised feeds and repeatedly exposed to users, which progressively broadens its reach beyond existing followers.[1136] This algorithmic amplification is reinforced by platform monetisation and optimisation mechanisms, including revenue-sharing models and engagement-based incentives that encourage the production of high-volume, attention-optimised content.[1137] Organic and paid distribution mechanisms also facilitate the diffusion of finfluencer content. Finfluencers make use of short-form videos, livestreams, stories, reels, and comment functions to present their content in

[1133] Interview 6; Antara Sen, Influence of Social Media and Finfluencers on Investor Behaviour (2026), available at: https://www.ijfmr.com/papers/2026/1/66685.pdf; Investigate Europe, The rogue 'finfluencers' pushing risky investments to young followers (2025), available at: https://www.investigate-europe.eu/posts/the-rogue-finfluencers-pushing-risky-investments-to-young-followers;

[1134] European Securities and Markets Authority (ESMA), Warning on Social Media and Investment Recommendations (2024), available at: https://www.esma.europa.eu/sites/default/files/2024-02/ESMA74-1103241886-912_Warnings_on_Social_Media_and_Investment_Recommendations.pdf.

[1135] European Parliament, Finfluencers: Setting Standards in a High-Risk Environment (2026), available at: https://www.europarl.europa.eu/news/en/agenda/plenary-news/2026-04-27/18/finfluencers-setting-standards-in-a-high-risk-environment.

[1136] Brandon Dulisse et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545; for a general analysis of recommender systems, see Katarzyna Szymielewicz, Reclaiming the Algorithm: What the DSA can—and can't—fix about recommender systems (2026), available at: https://dsa-observatory.eu/2026/02/15/reclaiming-the-algorithm-what-the-dsa-can-and-cant-fix-about-recommender-systems/.

[1137] ibid.

simplified and highly engaging formats.[1138] Some of these features are temporary in nature, limiting traceability once stories expire or livestreams conclude.[1139] These formats are designed to maximise attention and interaction, while often reducing the visibility of risk disclosures or contextual financial information.[1140]

Further, finfluencers may push users to migrate from online platforms into private communication channels. Within these environments, trust-building and persuasive communication can be intensified outside the reach of platform moderation systems, and users are subsequently redirected to external fraudulent websites.[1141] According to the German Financial Authority (BaFin), chat groups created by finfluencers can be associated with riskier investment behaviour, with evidence indicating significant differences in crypto-asset investment decisions between users who have access to such groups and those who do not.[1142]

Operational tools and behavioural models relevant to the scam

Firstly, finfluencer-related investment scams may operationalise through monetisation structures based on affiliate marketing and referral arrangements, where finfluencers receive commissions for directing users to financial products or services.[1143] These arrangements are often not transparent to end users and may create incentives to promote financial products irrespective of their risk profile or suitability, particularly where remuneration is linked to user registration, deposits, or trading activity.[1144] Alongside these incentivising structures, deceptive technical infrastructures support the scam, including cloned websites that imitate legitimate financial institutions or trading platforms with only minor variations in branding or domain names, as well as more advanced fake trading environments that simulate dashboards, transaction histories, and apparent investment returns to manufacture credibility.[1145]

[1138] Marius Mölders, Lennart Bock, Eloy Barrantes, and Henning Zülch, Understanding Finfluencers: Roles and Strategic Partnerships in Retail Investor Engagement (2025), available at: https://www.sciencedirect.com/science/article/pii/S0148296325002851.

[1139] Union des Fabricants (UNIFAB), Counterfeiting & Organised Crime (2025), available at: https://www.unifab.com/wp-content/uploads/2025/06/UNIFAB_Contrefacon-Criminalite_ENGLISH_VDEF_03062025.pdf.

[1140] Marius Mölders, Lennart Bock, Eloy Barrantes, and Henning Zülch, Understanding Finfluencers: Roles and Strategic Partnerships in Retail Investor Engagement (2025), available at: https://www.sciencedirect.com/science/article/pii/S0148296325002851.

[1141] Jingjia Xiao, Qing Xiao and Hong Shen, “It felt real” victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[1142] Bafin, Investment in cryptoassets and the influence of social media on investment behaviour (2026), available at: https://www.bafin.de/EN/die-bafin/publikationen-daten/risiken-im-fokus/Fokusrisiken_2026/RIF_Verbraucher_2/RIF_verbraucher_sozialemedien_en.html.

[1143] Federico Mangiò and Giandomenico Di Domenico, All that Glitters Is Not Real Affiliation: How to Handle Affiliate Marketing Programs in the Era of Falsity (2022), available at: https://www.sciencedirect.com/science/article/pii/S0007681322000775.

[1144] ibid.

[1145] Interview 4; Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”; Jingjia Xiao, Qing Xiao and Hong Shen, “It felt real” victim

Impersonation constitutes another key operational tool. Fraudsters may impersonate successful finfluencers, celebrities, financial professionals, or regulated financial institutions to legitimise investment offers.[1146] In parallel, synthetic social media personas may be created to establish credibility and develop parasocial relationships with users, thereby strengthening trust.[1147] These practices are increasingly reinforced through generative AI, including deepfake technologies used to fabricate endorsements, AI-generated promotional content, and voice cloning or conversational agents that simulate interactions with financial advisers or experienced investors.[1148]

Finally, the apparent legitimacy and popularity of financial content may be artificially enhanced through bot networks and coordinated inauthentic engagement. Automated accounts can inflate follower counts, generate comments, produce testimonials, and simulate participation within investment communities, thereby creating a misleading impression of widespread endorsement and success.[1149] Such systems are increasingly sophisticated and can generate realistic interactions that are difficult for users to distinguish from genuine engagement.[1150] The increasing commercial availability of such tools lowers barriers to entry for malicious actors and contributes to the persistence and scalability of inauthentic activity across online platforms.[1151]

perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[1146] ibid; Vilma Luoma-aho et al., Vulnerabilities to Crypto Currency Scams and Online Persuasion Strategies (2025), available at: https://jyx.jyu.fi/bitstreams/5459bc01-0ded-457b-b4ab-45617cbecc08/download; Xigao Li et al., Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams (2023), available at: https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_f584_paper.pdf.

[1147] Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/; Financial Services and Market Authority, Received an interesting credit offer? Be careful! (2025), available at: https://www.fsma.be/en/warnings/received-interesting-credit-offer-be-careful; Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en; Rajvardhan Oak and Zubair Shafiq, “Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf.

[1148] Interview 6; Watchlist Internet, Die Evolution des Online-Betrugs: Vom klassischen Internetbetrug zur KI-gestützten Täuschung (2024), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Bericht_KI_und_Betrug_final.pdf; ÖIAT, Dubiose Werbung auf Meta-Plattformen: Wie Celebrity-Ärzte zur Bewerbung von Nahrungsergänzungsmitteln missbraucht werden (2025), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Safe-NEM-Bericht.pdf.

[1149] Interview 8; Demagog, Metoda „na walizkę” – jak działają oszuści na Facebooku? (2024), available at: https://demagog.org.pl/analizy_i_raporty/jak-oszusci-z-cypru-okradaja-polakow-oto-historia-pani-iwony/.; Autorité des Marchés Financiers, Social Media Intelligence: Arnaques à l’investissement sur le web (2024), available at: https://www.amf-france.org/sites/institutionnel/files/private/2024-12/opinionway-pour-amf-les-arnaques-sur-le-web_octobre-2024_0.pdf; Dennis Assenmacher et al., Demystifying Social Bots: On the Intelligence of Automated Social Media Actors (2020), available at: https://journals.sagepub.com/doi/pdf/10.1177/2056305120939264; StreamCharts, The Hidden Cost of Viewbotting (2025), available at: https://streamscharts.com/reports/viewbotting-whitepaper.

[1150] ibid.

[1151] Interview 8.

In terms of behavioural tools, finfluencers leverage psychological levers, particularly the 'Fear Of Missing Out' (FOMO), to drive impulsive, emotionally driven investment decisions. Content often emphasises limited-time opportunities, early-access advantages, or imminent market movements, channelling users' aspirational goals into fast action.[1152] This is often combined with urgency and scarcity cues designed to compress decision-making time and discourage independent verification.[1153] This is done alongside social proof material where testimonials, follower engagement, profit screenshots, and community activity are used to create the perception that others have successfully benefited from the promoted opportunities.[1154] Overall, trust is gradually developed through repeated and consistent content exposure.

Platform-level interventions

None of the 2025 SRAs of the video-sharing platforms under the scope of this case study uses the specific term 'finfluencer'. However, they address the broader phenomena of fraudulent, deceptive, and scam-related advertising and commercial practices on video-sharing platforms, within which finfluencer-related investment scams would fall, and the following analysis draws on those findings.

At the preventive stage, platforms apply policies restricting the promotion of certain financial products and high-risk investment schemes. These policies vary across platforms. For example, Facebook and Instagram prohibit advertisements relating to financial products commonly associated with fraudulent activity;[1155] TikTok prohibits content promoting pyramid schemes, while also restricting the promotion of wealth-generation schemes that may present misleading returns;[1156] and X applies restrictions on investment-related advertising and wealth-generation content.[1157] Although these measures primarily apply to paid advertising, they are relevant to finfluencer activity where financial promotions occur through sponsorships, affiliate marketing, or commercial partnerships.[1158]

A second layer of intervention relates to content moderation and pre-publication review processes. According to their 2025 SRAs, all platforms mentioned above employ combinations of automated detection systems and human review to assess content and subsequently may restrict, suspend, or delete accounts or individual pieces of content. TikTok reports that it restricts the visibility of certain financial advertising to younger

[1152] Pooja Devi et al., Influencer or Finfluencer: A Comprehensive Study of Behavioural Financial in the Age of Digital Social Media (2026), available at: https://ieeexplore.ieee.org/abstract/document/11465570.

[1153] Jingjia Xiao, Qing Xiao and Hong Shen, "It felt real" victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[1154] ibid.

[1155] Meta, Advertising Standards, available at: https://transparency.meta.com/policies/ad-standards/.

[1156] TikTok, Deceptive Practices (2025), available at: https://ads.tiktok.com/help/article/tiktok-ads-policy-deceptive-practices.

[1157] X, Ads Policies: Deceptive & Fraudulent Content, available at: https://business.x.com/en/help/ads-policies.

[1158] Felix Pflücke, Regulating Influencers in the European Union: Current Challenges and Future Perspectives (2024), available at: https://www.cecluxembourg.lu/wp-content/uploads/5-Pflucke_influencers.pdf.

users.[1159] Further, Meta, TikTok, YouTube, Snapchat, and X reports that they provide channels for users to report fraudulent content, impersonation, or misleading financial promotions, including dedicated categories for scams and deceptive practices.[1160] TikTok and X also report implementing 'notice-and-action' reporting pathways for such content.[1161]

Transparency requirements regarding commercial relationships constitute another relevant area of intervention. All platforms report that they require varying levels of disclosure for sponsored content, affiliate links, or branded partnerships. Specifically, YouTube claims that it requires creators to declare paid promotions and displays an automatic disclosure message to viewers when content has been identified as containing paid product placements, sponsorships or endorsements, in accordance with applicable advertising disclosure requirements.[1162] Similarly, Facebook and Instagram provide tools that allow creators to label content involving paid partnerships.[1163] In parallel, platforms report the introduction of verification and traceability mechanisms aimed at strengthening account integrity and reducing impersonation. Facebook and Instagram maintain verification procedures for certain categories of official accounts associated with commerce and paid content.[1164] TikTok has implemented trader traceability measures and creator verification processes, including identity and age verification requirements in certain commercial contexts.[1165]

Limitations of current measures and systemic challenges identified

Despite the interventions described above, the 2025 SRAs of the relevant designated services acknowledge persistent systemic challenges in combating fraudulent and deceptive commercial practices.[1166] These systemic challenges identified relate to scams generally and do not specify finfluencer-related scams specifically.

Facebook's and Instagram's assessments identify scams and deceptive commercial practices as an evolving risk area.[1167] Snapchat likewise identifies scams, impersonation and deceptive commercial activity as persistent threats that require ongoing monitoring and adaptation of detection systems.[1168] TikTok highlights the challenges posed by

[1159] TikTok 2025 Systemic Risk Assessment Report.

[1160] Facebook, Instagram, TikTok, YouTube, Snapchat, and X 2025 Systemic Risk Assessment Reports.

[1161] TikTok and X, 2025 Systemic Risk Assessment Reports.

[1162] Google, Add paid product placements, sponsorships & endorsements, available at: https://support.google.com/youtube/answer/154235?hl=en; Google, Watching videos with paid product placements, sponsorships & endorsements, available at: https://support.google.com/youtube/answer/10588440?hl=en;

[1163] Meta, Branded Content, available at: https://creators.facebook.com/tools/branded-content/.

[1164] Meta, Protect your Brand with Meta Verified, available at: https://www.meta.com/en-gb/meta-verified/?srsltid=AfmBOool3T_ugNMKodDTmzqBymB_KGXNTIFuaJ6XP6dEd-7L3D_XG1w5.

[1165] TikTok 2025 Systemic Risk Assessment Report.

[1166] Facebook, Instagram, Google, TikTok, Snapchat and X 2025 Systemic Risk Assessment Reports.

[1167] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[1168] Snapchat 2025 Systemic Risk Assessment Report.

coordinated deceptive activity, impersonation and evolving manipulation techniques.[1169] X similarly identifies fraud, scams and platform manipulation as ongoing risks and acknowledges the need for continuous detection and enforcement efforts to respond to evolving abuse patterns.[1170] All cited platforms acknowledge that scammers are highly skilled in adapting their behaviour to platform enforcement mechanisms and increasingly exploit generative AI tools to scale deceptive activity and evade detection.

A further challenge identified across the reports concerns the persistence of residual exposure to fraudulent and deceptive content despite platform-level enforcement measures. Facebook and Instagram note that enforcement actions reduce the risk posed by adversarial actors but do not eliminate it, given that such actors continuously adapt their behaviour in response to platform interventions.[1171] Similarly, YouTube's assessment acknowledges that scams and fraudulent activity remain an evolving risk area.[1172]

A broader regulatory challenge concerns the position of finfluencers within a complex regulatory landscape governing financial information and advice, delivered on video-sharing platforms. While finfluencers increasingly influence retail investment behaviour across the European Union, their activities often blur the boundaries between financial education, personal opinion, commercial promotion, and investment recommendations and advice, leading to inconsistent identification, categorisation, and moderation by platforms.[1173] This creates an environment of regulatory ambiguity, cross-jurisdictional inconsistencies, and subsequently limited enforcement capacity in relation to finfluencer activity.[1174]

Conclusions and recommendations

This case study finds that finfluencer-related investment scams may be enabled by the convergence of platform design, creator monetisation, and the blurred boundary between financial education, entertainment, and promotion. On video-sharing platforms, recommendation systems and engagement-based ranking repeatedly surface aspirational financial content, while short-form videos, livestreams, comment functions, and private messaging channels make it easy to move users from public visibility into more persuasive and less accountable environments. These dynamics are reinforced by platform monetisation models that incentivise sponsorships, affiliate marketing, referrals, and other forms of commercial engagement.

The particularity of finfluencer-related investment scams lies in the role of finfluencers themselves, who may act as deliberate perpetrators of fraud, negligent promoters of high-risk financial products, or unwitting intermediaries exploited by fraudulent actors. Where finfluencers knowingly or unknowingly facilitate deceptive investment schemes,

[1169] TikTok 2025 Systemic Risk Assessment Report.

[1170] X 2025 Systemic Risk Assessment Report.

[1171] Facebook, Instagram 2025 Systemic Risk Assessment Report.

[1172] Google 2025 Systemic Risk Assessment Report.

[1173] Essam Ghadafi and Panagiotis Andriotis, UK Finfluencers: Exploring Content, Reach, and Responsibility (2025), available at: https://arxiv.org/abs/2505.01941.

[1174] Henning Zülch, Marius Mölders, and Christian Pieter Hoffmann, Navigating the Rise of Finfluencers: A Multidimensional Quality Framework for Strategic Partnerships (2026), available at: https://link.springer.com/article/10.1057/s41264-025-00334-7.

consumers may be exposed to undisclosed commercial relationships, misleading endorsements, impersonation of legitimate financial professionals or institutions, cloned investment platforms, coordinated inauthentic engagement, and increasingly AI-generated content that enhances the credibility and scalability of fraudulent investment promotions.

Regulatory attention towards finfluencer activity is increasing at both national and EU levels, reflecting growing recognition that financial influence on video-sharing platforms occupies a regulatory grey area. The boundaries between commercial communications, investment recommendations, investment advice, financial education, and personal opinion are often difficult to distinguish in practice, making it challenging for platforms, regulators, and consumers to determine which legal obligations apply and whether misleading conduct constitutes unlawful financial promotion or outright fraud. This complexity is compounded by the uncertain legal status of finfluencer activity within the existing EU consumer and financial regulatory framework and by the diversity of roles that finfluencers may assume, ranging from deliberate perpetrators of investment scams to negligent promoters of high-risk financial products or unwitting intermediaries exploited by fraudulent actors.

Alongside regulatory initiatives, industry self-regulation provides practical measures to promote responsible influencer marketing. The European Advertising Standards Alliance (EASA) Best Practice Recommendation on Influencer Marketing recommends that commercial relationships be clearly identifiable through prominent, immediate disclosure, regardless of the platform or content format used. It further emphasises the shared responsibility of influencers, advertisers, agencies, and platforms to ensure that advertising is transparent and compliant with applicable consumer protection rules through contractual arrangements, monitoring, and effective complaint-handling mechanisms.[1175] Complementing these recommendations, EASA has developed dedicated training for influencers to improve their understanding of advertising rules, disclosure obligations, and responsible commercial practices, helping content creators recognise when commercial communications require transparency and how to comply with applicable legal and ethical standards.[1176] Complementing these regulatory measures, stakeholders recommend that platforms could adopt a risk-based approach to detecting and moderating finfluencer-related investment scams by distinguishing between different patterns of financial promotion and associated levels of consumer risk.[1177] Detection systems could combine indicators such as the absence of legally required disclosures, repeated promotion of high-risk financial products, undisclosed commercial relationships, and links to unregulated or fraudulent investment services to differentiate between potentially negligent conduct and deliberate fraudulent activity, thereby enabling more proportionate and effective enforcement.[1178]

[1175] European Advertising Standards Alliance (EASA), EASA Best Practice Recommendation on Influencer Marketing Guidance 2023 (2023), available at: https://www.easa-alliance.org/publications/best-practice-recommendation-on-influencer-marketing-guidance_v2023/.

[1176] European Advertising Standards Alliance (EASA), Responsible influencer marketing, available at: https://www.easa-alliance.org/responsible-influence/.

[1177] Multi-stakeholder Workshop on Online Financial Scams.

[1178] ibid.

6.2. Case study B: Romance baiting scams on social media platforms

Purpose of the case study

Romance baiting, as defined in Section 2.2.2, is a hybrid scam typology that combines the long-term trust-building model of romance scams with the financial extraction mechanisms of investment fraud. This scam type has been selected as representative of a broader trend towards the hybridisation of online scams, whereby offenders combine behavioural, operational, and technical elements traditionally associated with distinct scam typologies into a single criminal scheme.

Scope and methodology

This case study prioritises social media platforms hosting and amplifying romance baiting scams. It examines how platform design shapes exposure to romance baiting scams. The case study considers the services provided by Facebook and Instagram (Meta), Snapchat, TikTok, and X as part of the scope.

Methodologically, the study triangulates (i) DSA materials, including VLOP/VLOSE risk assessment reports, enforcement actions and the DSA Transparency Database; (ii) regulatory alerts and enforcement by national consumer/product-safety authorities; (iii) academic literature and investigative reporting on romance baiting; (iv) targeted interview data from Tasks 1 and 2; (v) the case study findings as explored and validated through the workshop (Task 4).

Background on scam model, prevalence and impact

As described in Section 2.2., romance baiting emerged from a growing global convergence between romance scams and investment scams since 2019.[1179] Once victims have invested significant amounts, offenders may continue to manipulate them into making further payments or abruptly terminate contact.

Romance baiting combines elements of traditional romance scams with investment scams, reflecting the ongoing evolution of scam methodologies aimed at increasing effectiveness and circumventing existing prevention and detection measures.[1180] Unlike traditional romance scams, where emergencies or personal crises commonly justify requests for money, romance baiting relies on persuading victims to participate in an ostensibly legitimate investment opportunity for their own benefit.[1181] The investment proposal is embedded within the established relationship and frequently linked to narratives about a shared future, financial security, or mutual prosperity.[1182] For a detailed description of the trust-building techniques employed, see Section 3.2.5.

[1179] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025 (2025), available at: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

[1180] ibid.

[1181] Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670.

[1182] ibid.

Victims of romance baiting scams are more often in a younger age group compared to traditional romance scams.[1183] One piece of evidence suggests that individuals aged 25 to 34 are particularly affected, especially those with higher levels of education and familiarity with digital technologies.[1184] Others suggest that romance baiting does not show a pronounced age skew. Instead, victims are often defined more by situational drivers such as financial aspirations and interest in cryptocurrency markets.[1185] Scammers may often try to re-target victims through secondary scams after the initial scam, exploiting victims' desperation to recover their losses.[1186]

Romance baiting is predominantly operated by organised cybercrime networks that operate across multiple jurisdictions.[1187] Evidence suggests that many large-scale operations are concentrated in the ASEAN region, as well as mainland China, Hong Kong, Taiwan, Africa and Latin America (see Section 3.2.6 for a cross-cutting analysis of organised crime infrastructure, including scam compounds and the intersection with human trafficking). In late 2024, more than two million accounts linked to romance baiting activity were reportedly removed by major online platforms, including Meta, with activity associated not only with criminal centres in Southeast Asia but also with emerging operations in Eastern Europe and Africa.[1188]

In terms of prevalence, according to Chainalysis, in 2024, romance baiting grew by almost 40% year-on-year, reportedly generating between EUR 9.1 (USD 10.6) billion and EUR 11.4 (USD 13.3) billion, and accounting for over one-third of global cryptocurrency scam revenue.[1189] Further, between 10 and 17 September 2024, Europol coordinated an international operation dismantling a mobile-phone phishing network that unlocked over 1.2 million stolen devices, where elements of the compromised devices and stolen credentials had been repurposed for romance baiting outreach and cryptocurrency theft.[1190] In 2025, in Malta, the Office of the Arbiter for Financial Services

[1183] ibid.

[1184] ibid.

[1185] Fangzhou Wang, A scoping review of online romance scams: Conceptual construction and comparative analysis (2026), available at: https://journals.sagepub.com/doi/pdf/10.1177/02697580251414141.

[1186] Rajvardhan Oak and Zubair Shafiq, "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf; Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670.

[1187] Rajvardhan Oak and Zubair Shafiq, "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf; https://fr.tenable.com/blog/pig-butchering-scam-tinder-tiktok-whatsapp-telegram-scammers-steal-millions

[1188] Meta, Cracking Down on Organised Crime Scam Centres (2024), available at: https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/; European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025 (2025), available at: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

[1189] Chainalysis, The Rise of Pig Butchering Scams: Revenue Growth and Criminal Ecosystems (2024), available at: https://www.chainalysis.com/blog/2024-pig-butchering-scam-revenue-grows-yoy/.

[1190] Europol, Criminal Phishing Network Resulting in Over 480,000 Victims Worldwide Busted in Spain and Latin America (2024), available at: https://www.europol.europa.eu/media-

was approached by complainants who had suffered significant losses from romance baiting scams ranging from low five-digit to high six-digit figures.[1191]

The dual nature of romance baiting amplifies its overall impact. Victims are not only subject to financial exploitation but also experience the perceived loss of a trusted personal or romantic relationship. As these scams typically unfold over extended periods, the emotional investment made by victims can reinforce the deception and contribute to both substantial financial losses and enduring psychological harm.[1192] Financial consequences may include the loss of savings, the accumulation of debt, and the liquidation of assets. In some cases, victims take out personal loans or borrow money from friends and family in order to make additional investments under the offender's influence.[1193] These losses can extend beyond the individual victim, creating wider financial consequences for dependents and family members.[1194] The emotional and psychological impact can be equally significant. Victims frequently report feelings of shame, embarrassment, self-blame, and a loss of trust in others.[1195] Research and victim accounts have also documented longer-term effects, including emotional distress, anxiety, depression, hypervigilance, and symptoms consistent with post-traumatic stress disorder.[1196]

Relevance to EU citizens and regulatory priorities

Romance baiting scams are increasingly reported as being leveraged to target citizens in the EU.[1197] Europol identifies romance scams and investment scams among the principal online scam threats affecting millions of victims across the EU and has published dedicated guidance warning users to recognise scams.[1198]

press/newsroom/news/criminal-phishing-network-resulting-in-over-480-000-victims-worldwide-busted-in-spain-and-latin-america.

[1191] Financial Arbiter of Malta, Technical Note – Follow Up (January 2026), available at: https://financialarbiter.org.mt/sites/default/files/Technical%20Note%20-%20Follow%20Up%20-%20Jan%202026%20%5BFinal%5D_0.pdf.

[1192] Bhupendra Acharya and Thorsten Holz, An Explorative Study of Pig Butchering Scams (2024), available at: https://arxiv.org/pdf/2412.15423.

[1193] Rajvardhan Oak and Zubair Shafiq, "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf; Bhupendra Acharya and Thorsten Holz, An Explorative Study of Pig Butchering Scams (2024), available at: https://arxiv.org/pdf/2412.15423; https://commons.erau.edu/cgi/viewcontent.cgi?article=3514&context=publication.

[1194] ibid.

[1195] ibid.

[1196] ibid.

[1197] European Union Agency for Cybersecurity (ENISA), ENISA Threat Landscape 2025 (2025), available at: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

[1198] Europol, Fragmented and multiplied cybercriminal landscape, warns new Europol report (2024), available at: https://www.europol.europa.eu/media-press/newsroom/news/fragmented-and-multiplied-cybercriminal-landscape-warns-new-europol-report; Europol, Romance scams: recognising manipulation before it escalates (2026), available at: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/romance-scams-recognising-manipulation-it-escalates.

Description of platform features relevant to scam propagation

Romance baiting generally begins on social media platforms, which provide offenders with access to large and continuously replenished pools of potential victims.[1199] Scammers leverage recommendation systems, including profile suggestions, follower recommendations, and content discovery tools, to identify users who may be receptive to contact.[1200] Public profile information, friend networks, follower lists, and contact synchronisation functions can provide valuable insights into a victim's social environment, personal interests, relationships, and socioeconomic circumstances. This information enables offenders to tailor their fictitious identities and communication strategies to specific target groups. Messaging functionalities available on social media platforms, including direct messages, voice notes, photo sharing, and persistent chat histories, further support the initial stages of relationship-building by enabling frequent and increasingly personalised interactions.[1201]

Once initial contact has been established, offenders typically encourage victims to migrate to private messaging services.[1202] This transition represents a critical stage in the scam. Moving the interaction away from public platforms reduces the likelihood that scam accounts will be reported or removed and allows offenders to operate in less moderated environments.[1203] Messaging services provide the private, continuous communication channels necessary to cultivate emotional intimacy, sustain prolonged engagement, and intensify manipulation.[1204] In other words, they create a 'dark space' for social engineering, largely outside the reach of automated monitoring or regulatory oversight.[1205]

The final stage of the scam typically involves redirecting victims towards fraudulent investment infrastructure. While fake trading websites remain common, fraudsters increasingly rely on application stores to distribute fraudulent investment applications

[1199] Satnam Narang, Pig Butchering Scam: From Tinder and TikTok to WhatsApp and Telegram, How Scammers Are Stealing Millions in a Long Con (2024), available at: https://www.tenable.com/blog/pig-butchering-scam-tinder-tiktok-whatsapp-telegram-scammers-steal-millions; Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670.

[1200] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA"; Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670; Jingjia Xiao, Qing Xiao and Hong Shen, "It felt real" victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680.

[1201] ibid.

[1202] Janneke M Schokkenbroek and Thom Snaphaan, Love as Bait: A Scoping Review and Crime Script Analysis of Online Romance Scams (2025), available at: https://journals.sagepub.com/doi/10.1177/15248380251361046.

[1203] Interviews 4, 5.

[1204] Interview 4.

[1205] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

that can be accessed by victims across multiple jurisdictions and languages.[1206] These false investment apps often impersonate legitimate financial institutions or offer fake high-yield trading opportunities, sometimes showing fake profits to encourage further, larger deposits before locking users out.[1207]

Operational tools and behavioural models relevant to the scam

The foundational operational tool of romance baiting scams is impersonation, namely the creation of fictitious romantic or social personas to establish emotional relationships with victims.[1208] To enhance the credibility of these identities, offenders may use stolen photographs and personal information or generate synthetic content using AI. As offenders frequently manage multiple victims simultaneously, they may also operate networks of fake profiles and use AI-generated images, videos, and messages to reinforce the authenticity of their online personas and maintain engagement over extended periods.[1209] Once directed outside social media platforms, victims are exposed to fraudulent websites or applications that imitate legitimate investment services.[1210] Fraudsters may also circulate links to fraudulent websites, crypto wallets, payment instructions, QR codes, and other materials required to facilitate financial transactions.[1211] Document sharing, media attachments, and video calls further enable scammers to distribute fabricated investment statements, fake documentation, and, increasingly, to use AI-enabled tools such as deepfakes to conceal their identities during video interactions.[1212] Finally, advance-fee mechanisms are also used in romance baiting operations. Once victims believe that profits have been generated, they may be informed that further payments are required before funds can be released.[1213] These payments are often presented as taxes, regulatory charges, anti-money laundering checks, transaction processing fees, or account verification requirements.

Romance baiting relies on the behavioural manipulation techniques described in Section 3.2.5, designed to establish trust, create a sense of legitimacy, and reduce victims' ability

[1206] Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024) available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en.

[1207] ibid.

[1208] Rajvardhan Oak and Zubair Shafiq, “Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf.

[1209] Interview 8; Autorité des Marchés Financiers, Social Media Intelligence: Arnaques à l’investissement sur le web (2024), available at: https://www.amf-france.org/sites/institutionnel/files/private/2024-12/opinionway-pour-amf-les-arnaques-sur-le-web_octobre-2024_0.pdf; Dennis Assenmacher et al., Demystifying Social Bots: On the Intelligence of Automated Social Media Actors (2020), available at: https://journals.sagepub.com/doi/pdf/10.1177/2056305120939264; StreamCharts, The Hidden Cost of Viewbotting (2025), available at: https://streamscharts.com/reports/viewbotting-whitepaper.

[1210] Rajvardhan Oak and Zubair Shafiq, “Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf.

[1211] ibid, Interview 4.

[1212] ibid.

[1213] Alexander Bilz et al., Tainted Love: a Systematic Literature Review of Online Romance Scam Research (2023), available at: https://academic.oup.com/iwc/article/35/6/773/7331428.

to critically assess information and requests.[1214] The objective is to cultivate a relationship in which financial requests or investment opportunities are perceived as credible and consistent with the trust that has been established.[1215] Specifically, through techniques commonly associated with grooming and social engineering, offenders seek to establish rapport by mirroring the victim's values, preferences, and behaviours.[1216] This creates the impression of a genuine personal connection and exploits psychological principles such as trust, reciprocity, and social validation.[1217]

Platform-level interventions

None of the 2025 SRAs from the platforms under the scope of this case study specifically references the term 'romance baiting'. However, reports address the broader phenomena of fraudulent, deceptive, and scam-related content, and the following analysis draws on those findings.

Several platforms have implemented identity verification and account integrity measures. According to Facebook' and Instagram's SRAs, users may be required to submit identity documentation where suspicious activity is detected, and the platform employs systems designed to identify attempts by previously removed threat actors to create new accounts.[1218] Additional verification measures, including login challenges and contact-point verification, are also mentioned as tools to reduce account abuse.[1219] According to Snapchat's Report, Snapchat requires users to provide account registration information, including a username, date of birth, and a phone number and/or email address.[1220] Snapchat is currently exploring additional identity verification methods, including biometric verification, identity document scans, and financial transaction-based verification.[1221]

Since romance baiting relies on coordinated activity, platforms deploy a combination of automated detection systems and human review processes to identify fake profiles, impersonation, coordinated scam networks, and suspicious behavioural patterns. The 2025 SRAs of the relevant platforms under this case study indicate employing machine learning models, image and keyword detection, behavioural analysis, contextual review processes, and coordinated activity detection systems to identify potentially harmful

[1214] Cassandra Cross, Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670.

[1215] Which?, The psychology of scams, Understanding why consumers fall for APP scams (2022), available at: https://media.product.which.co.uk/prod/files/file/gm-c66f3d70-3928-4dee-bb8b-481405be2b5e-the-psychology-of-scams-understanding-why-consumers-fall-for-app-scams.pdf.

[1216] Sharon L. Burton and Pamela D. Moore, Pig Butchering in Cybersecurity: A Modern Social Engineering Threat (2024), available at: https://commons.erau.edu/publication/2266.

[1217] ibid.

[1218] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[1219] Meta, Learn about ID verification for Meta accounts (2026), available at: https://www.meta.com/en-gb/help/quest/1266914157405903/.

[1220] Snapchat 2025 Systemic Risk Assessment Report.

[1221] ibid.

activity.[1222] Facebook and Instagram additionally report that organised scam operations may be addressed through their Dangerous Organisations and Individuals framework, under which designated entities are removed from the platform and subjected to enhanced enforcement measures.[1223] These platforms also report that investigative teams monitor designated entities for attempts to re-establish their presence online and share threat intelligence with external stakeholders to support broader disruption efforts.[1224]

Several platforms report implementing user awareness measures designed to help users recognise suspicious interactions and common scam tactics. Meta states that it has introduced warnings in Messenger and Instagram direct messages to alert users to potentially suspicious interactions or unsolicited contact from unknown individuals.[1225] According to its SRA, TikTok reports that it operates a Safety Centre as a public-facing resource hub, including dedicated resources on online safety, digital wellbeing, and online scams.[1226]

User reporting mechanisms constitute an additional layer of defence against romance baiting by enabling users to flag suspicious profiles, impersonation attempts, fraudulent investment solicitations, and scam-related communications. Meta claims to operate reporting mechanisms across Facebook and Instagram that allow users to report content, profiles, pages, advertisements, and other account activity.[1227] However, the effectiveness of these mechanisms is currently subject to regulatory scrutiny. In its preliminary findings under the Digital Services Act, the European Commission expressed concerns that Meta's notice-and-action mechanism may not be sufficiently accessible or user-friendly and that aspects of its content moderation appeals process may not enable users to effectively challenge moderation decisions.[1228] These findings remain preliminary and do not prejudge the outcome of the Commission's investigation. Further, Facebook indicates that it includes dedicated reporting categories for scams, fraud, impersonation, and fake accounts, while Instagram addresses such content through its framework on deceptive and misleading content.[1229] Snapchat states that it provides both an in-app reporting system and a web-based reporting form accessible to users and non-users alike, including a dedicated category for fraud and spam.[1230] TikTok holds that it enables users to report videos, accounts, comments, and livestreams through in-app

[1222] Facebook, Instagram, Snapchat, TikTok 2025 Systemic Risk Assessment Reports.

[1223] Meta, Cracking Down on Organised Crime Scam Centres (2024), available at: https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/.

[1224] Ibid.

[1225] ibid.

[1226] TikTok 2025 Systemic Risk Assessment Report.

[1227] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[1228] European Commission, Commission preliminarily finds TikTok and Meta in breach of their transparency obligations under the Digital Services Act (2025), available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503

[1229] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[1230] Snapchat 2025 Systemic Risk Assessment Report.

reporting tools.[1231] X points towards its dedicated reporting mechanisms for illegal content and separate appeal procedures for content moderation decisions.[1232]

Limitations of current measures and systemic challenges identified

Despite the interventions described above, the 2025 SRAs acknowledge persistent systemic challenges in addressing scams generally.

Facebook's and Instagram's assessments identify scams, impersonation and coordinated inauthentic behaviour as evolving risks, noting that organised threat actors frequently adapt their tactics and re-establish accounts following enforcement actions, which limits the effectiveness of account removal and disruption measures over time.[1233] TikTok similarly highlights that scam actors continuously evolve their behavioural patterns and exploitation strategies, requiring ongoing adaptation of detection systems and enforcement tools to address increasingly sophisticated forms of deceptive engagement and impersonation.[1234] Snapchat's assessment also recognises impersonation, fraud and spam as persistent risks within its ecosystem, emphasising the need for continuous monitoring and iterative improvements to detection and reporting systems in response to evolving abuse techniques.[1235] X identifies platform manipulation, impersonation and scam-related activity as ongoing risks, requiring continuous enforcement and signalling that malicious actors often operate in coordinated and adaptive ways that are difficult to fully eradicate.[1236]

Conclusions and recommendations

This case study finds that romance baiting scams reach consumers through a chain of social media platform features that facilitate each stage of the scam, from victim identification and trust-building to migration into private communication channels and eventual financial exploitation through fraudulent investment infrastructure. Recommendation systems, profile discovery tools, and publicly available user information enable offenders to identify and approach potential victims, while direct messaging, voice notes, photo sharing, and persistent chat functions support prolonged relationship-building. Once trust has been established, victims are encouraged to move to less moderated messaging services, where emotional manipulation can be intensified before they are redirected to fraudulent trading platforms or investment applications. Offenders reinforce this process through impersonation, AI-generated personas and deepfakes, coordinated fake accounts, and fabricated investment materials, exploiting behavioural mechanisms such as trust, reciprocity, social validation, and emotional dependency. The case study further demonstrates that romance baiting reflects the growing hybridisation and industrialisation of online scams, combining techniques traditionally associated with romance fraud, investment fraud, and cyber-enabled deception within highly organised transnational criminal networks that continuously adapt their methods in response to platform interventions.

[1231] TikTok 2025 Systemic Risk Assessment Report.

[1232] X 2025 Systemic Risk Assessment Report.

[1233] Facebook, Instagram 2025 Systemic Risk Assessment Reports.

[1234] TikTok 2025 Systemic Risk Assessment Report.

[1235] Snapchat 2025 Systemic Risk Assessment Report.

[1236] X 2025 Systemic Risk Assessment Report.

Stakeholders consulted as part of this study recommend that platforms could strengthen the detection of romance baiting by incorporating behavioural risk indicators into their automated detection systems.[1237] In addition to content-based signals, these systems could consider anomalous account characteristics and behavioural patterns, such as unusual interaction networks, account age, and inconsistencies between profile attributes and observed activity, to identify potentially fraudulent accounts before they establish prolonged contact with users.[1238]

6.3. Case study C: Fake webshop advertisement on search engines

Purpose of the case study

Non-delivery scams and counterfeit scams executed through fake webshops are amongst the most prevalent categories of online financial scams, as reported in the survey by multiple national authorities.[1239] Although fake webshops are promoted through multiple dissemination channels, search engines play a structurally distinctive role in the reach of these scams by providing both paid advertising placements and organic discovery pathways. This topic has been chosen as an avenue for exploring the interaction between paid advertising and organic search manipulation.

Scope and methodology

This case study prioritises search engines that host and advertise fake webshops. It examines how search engines' design, indexing and algorithmic ranking systems, and advertising systems shape exposure to fake webshops. The case study considers the services provided by Bing and Google Search as part of the scope.

Methodologically, the study triangulates (i) DSA materials, including VLOP/VLOSE risk reports, enforcement actions and the DSA Transparency Database; (ii) regulatory alerts and enforcement by national consumer/product-safety authorities; (iii) academic literature and investigative reporting on fake webshops; (iv) targeted interview data from Tasks 1 and 2; (v) the case study findings, as explored and validated through the workshop (Task 4).

Background on scam model, prevalence and impact

As defined in Section 2.3.1, fake webshops or ghost stores involve fraudsters operating fraudulent online storefronts that advertise products or services, typically at implausibly low prices, collect advance payments, and then either fail to fulfil the contract (non-delivery scams) or provide fake products (counterfeit scams). The operational infrastructure underlying these scams is analysed in Section 3.2.3.

[1237] Multi-stakeholder Workshop on Online Financial Scams.

[1238] ibid.

[1239] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

Non-delivery scams and counterfeit scams are often perpetrated by criminal networks operating under an 'infrastructure-as-a-service' model, as described in Section 3.2.6.[1240]

Fake webshops have been identified by 11 Member States as one of the most common manifestations of online scams.[1241] According to the Eurobarometer survey (November 2025), conducted on behalf of the European Union Agency for Fundamental Rights (FRA) with 26,453 respondents across all 27 Member States, the most prevalent type of scam is being 'defrauded by someone pretending to sell goods or services,' experienced by 35% of all online-fraud victims.[1242] Expressed as a proportion of the general EU population, this corresponds to approximately 8% of people in the EU having been defrauded in this manner over their lifetime.[1243] In this context, it should be noted that the FRA survey category 'someone pretending to sell goods or services' is broader than the specific phenomenon of fake webshops examined in this case study. The category encompasses any fraud in which the perpetrator purported to offer goods or services that were paid for but never delivered, or where personal data were extracted under such a pretext.[1244]

As noted in Section 3.1.1, vzbv research shows that 50% of monitored fake webshops were advertised via Google's or Meta's designated services, with the five most wide-reaching shops alone generating 134 million ad impressions on Google platforms.[1245] The Dutch national hotline for online scams (LMIO) expected approximately 14,000 reports in 2023 concerning online stores that failed to deliver purchased items.[1246]

Watchlist Internet has documented this phenomenon at the national level.[1247] In its study 'Wege in Fake-Shops' (Paths into Fake Shops), Watchlist Internet found that 33.1% of victims who reported falling for a fake webshop had found the fraudulent site via Google (through Google Search, Google Image Search, or Google Shopping), making Google the single largest referral channel to fake shops.[1248] A further 20.9% of victims identified generic internet search as their route, a share that Watchlist Internet considers largely attributable to Google Search given its dominant market position in the DACH region

[1240] Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar.

[1241] ibid.

[1242] European Union Agency for Fundamental Rights (FRA), Online Fraud – People's experiences across the EU (2026), available at: https://fra.europa.eu/en/publication/2026/victims-online-fraud.

[1243] ibid.

[1244] ibid.

[1245] Verbraucherzentrale Bundesverband, Jeder zweite Fakeshop schaltet Werbung auf Google oder Meta (2025), available at: https://www.vzbv.de/pressemitteilungen/jeder-zweite-fakeshop-schaltet-werbung-auf-google-oder-meta.

[1246] Autoriteit Consument en Markt, Consumer organizations warn against untrustworthy online stores (2023), available at: https://www.acm.nl/en/publications/consumer-organizations-warn-against-untrustworthy-online-stores.

[1247] Watchlist Internet, "Wege in Fake-Shops" (Paths into Fake Shops), available at: https://www.watchlist-internet.at/news/wege-in-fake-shops/.

[1248] ibid.

(Germany, Austria, Switzerland).[1249] Additionally, Google states in its 2025 Ads Safety Report that it blocked or removed more than 8.3 billion ads and suspended 24.9 million advertiser accounts, including some 602 million scam ads.[1250]

In terms of financial loss, the Dutch Fraud Help Desk data cited in Section 3.5 indicates that the average financial harm from fake webshop scams reached approximately EUR 350 per victim in 2023.[1251] However, the aggregated financial loss ranks highly, particularly considering the high volume of scams. For example, the BogusBazaar operation alone processed over USD 50 million (approx. EUR 43 million) in fake orders between 2021 and 2024.[1252]

Beyond direct financial loss, victims may face secondary harm from the subsequent exploitation of stolen payment data for further fraudulent transactions. The difficulty of obtaining recourse once a payment has been made to a fraudulent site is a consistent feature of victim experiences, and a structural challenge for enforcement.[1253]

Relevance to EU citizens and regulatory priorities

Fake webshop advertisements are highly relevant to EU citizens because they sit at the intersection of three large-scale EU policy priorities: consumer protection, the integrity of online advertising, and trust in cross-border e-commerce. Google Search alone reports more than 364 million EU users.[1254] The consumer detriment is correspondingly broad: fake webshop ads can cause direct financial loss, exposure of payment and identity data, non-delivery of goods, purchase of counterfeit or unsafe products, and erosion of confidence in legitimate online commerce. They also create a competition and Single Market concern by diverting demand away from compliant traders and by exploiting advertising and ranking systems to give fraudulent merchants the appearance of legitimacy.

With the DSA, the EU regulatory response requires VLOPs and VLOSEs to assess and mitigate systemic risks, including risks linked to illegal content, consumer protection, deceptive design, and advertising systems; it also imposes due-diligence obligations relevant to advertising transparency, trader traceability, notice-and-action, risk mitigation, independent audit, and researcher or regulatory scrutiny. At the consumer-

[1249] ibid.

[1250] Memyco, Fake Search Ads and Brand Impersonation: Why Takedown Alone Misses the Real Risk (2026), available at: https://www.memcyco.com/fake-search-ads-brand-impersonation; Malwarebytes, Malvertising via brand impersonation is back again (2023), available at: https://www.malwarebytes.com/blog/threat-intelligence/2023/05/malvertising-its-a-jungle-out-there.

[1251] Autoriteit Consument en Markt, Consumer organizations warn against untrustworthy online stores (2023), available at: https://www.acm.nl/en/publications/consumer-organizations-warn-against-untrustworthy-online-stores.

[1252] Business Insider, A Chinese criminal ring has stolen $50 million by franchising thousands of fake online shops, experts say (2024), available at: https://www.businessinsider.com/fake-online-shops-china-crime-ring-franchise-model-target-americans-2024-5.

[1253] ECC-Net, Fraud in Cross-border E-commerce (2016), available at: https://www.eccnet.eu/publication/online-fraud; Survey among national authorities on “Scoping of the National Online Fraud Landscape in the EU Member States under the DSA”.

[1254] European Commission, Supervision of the designated very large online platforms and search engines under DSA, available at: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-google.

law level, the Consumer Protection Cooperation (CPC) Network coordinates national enforcement authorities to conduct EU-wide 'sweeps' of online markets and require corrective action from traders.[1255] Furthermore, the European Consumer Centres Network (ECC-Net) offers EU residents and citizens advice on their consumer rights and legal protections when shopping in another European Union Member State, Norway or Iceland.[1256] These initiatives are relevant because fake webshops rarely operate as purely local problems; they can target consumers across Member States, disappear quickly, reappear under new domains or trader identities, and exploit gaps between platform moderation, payment systems, hosting services, and national enforcement.

Description of search engine features relevant to scam propagation

Search engines combine multiple functionalities that, individually and collectively, create opportunities for fake webshop operators to reach consumers. This section examines the specific platform features through which fraudulent shops gain visibility. A search engine typically combines 'organic' results, which depend on the query and the ranking of indexed websites, with 'paid for' results and ads, which are based on the user's query, profile and behaviour together with advertiser ad inventories; although visually separated on the results page, the two are blended into a single search experience.[1257]

As also highlighted in the section above, paid advertising is the dominant dissemination channel for fake webshops.[1258] The prevalent business model of major search engines generates revenue from advertising, whereby paid ads and sponsored links are sold to advertisers and displayed alongside organic results.[1259] Access to this inventory is mediated by an auction: advertisers bid on keywords that match users' search terms, and a successful bid places the ad against a given query, subject only to a contractual relationship between the search engine and the advertiser rather than the editorial vetting applied to hosted content.[1260]

Operators of illegitimate sites misuse this channel, known as Search Engine Marketing (SEM), by bidding on brand names and other high-relevance keywords and by deploying misleading or deceptive ads that impersonate an official web store or make unauthorised use of trademarks to funnel users to infringing or fraudulent destinations.[1261]

The placement of advertisements within search results pages is also a factor in determining consumer exposure to fake webshops. Sponsored links are structured like

[1255] European Commission, Consumer Protection Cooperation Network, available at: https://commission.europa.eu/topics/consumers/consumer-rights-and-complaints/enforcement-consumer-protection/consumer-protection-cooperation-network_en.

[1256] European Consumer Centres Network, Advice and assistance for consumers in the EU, Norway and Iceland, available at: https://www.eccnet.eu/.

[1257] EUIPO, Search Engines – Challenges and Good Practices to Limit Search Traffic (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf.

[1258] ibid.

[1259] ibid.

[1260] ibid.

[1261] ibid.

organic results (headline, URL and description) and are typically embedded on the first page among the organic listings, while banner and shopping ads are shown at the top, side or bottom of the results page.[1262] Because the highest-value placements sit at the very top of the page, an ad occupying that prime position inherits a 'credibility boost' that fraudulent operators exploit, and the practical difficulty of distinguishing sponsored from organic content is acute on mobile, where the two content types sit side by side on limited screen space.[1263]

Placement is also personalised: ads, like organic results, are tailored to a user's search history, location or profile, so different users may see different ads for the same query, a dynamic the EUIPO identifies as making it difficult for rights holders and investigators to reproduce and monitor infringing placements.[1264] Security vendors report that threat actors reinforce this evasiveness by serving unique session cookies and geo- or user-agent-targeted variants so that automated scanners see benign pages while victims are routed to phishing or fake-shop destinations.[1265]

Watchlist Internet's reporting reinforces this point with specific examples. In its analysis of fake-shop trends, Watchlist Internet documented that when consumers used Google Search to look for a common household product such as a washing machine, Google Ads displayed advertisements for fraudulent shops among the results, illustrating how paid placement directly delivers scam exposure during routine consumer searches.[1266] A joint investigation by the Vienna Chamber of Labour (Arbeiterkammer Wien, AK Wien) and Watchlist Internet further showed how quickly consumers encounter fraudulent advertisements: using three separate user profiles, researchers queried Google Search for up to one hour and found that most of the shops surfaced through advertising were in fact untrustworthy dropshipping operations or outright fake shops.[1267]

Beyond paid advertising, fake webshops also exploit organic search indexing and ranking systems to gain visibility. Search engines use automated crawlers to discover and index web pages, and employ complex ranking algorithms to determine the order in which results appear for any given query.[1268] Operators of fraudulent and infringing sites

[1262] ibid.

[1263] WIRED, Malicious Ads in Search Results Are Driving New Generations of Scams (2024), available at: https://www.wired.com/story/malicious-ads-in-search-results-are-driving-new-generations-of-scams.

[1264] EUIPO, Search Engines – Challenges and Good Practices to Limit Search Traffic (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf.

[1265] BlueVoyant, The rising Threat of Search Engine Ad Abuse (2024), available at: https://www.bluevoyant.com/blog/the-rising-threat-of-search-engine-ad-abuse.

[1266] Watchlist Internet, Trends und Entwicklungen bei Fake-Shops, available at: https://www.watchlist-internet.at/news/trends-und-entwicklungen-bei-fake-shops/.

[1267] Watchlist Internet, Vorsicht vor Werbung unseriöser Online-Shops!, available at: https://www.watchlist-internet.at/news/vorsicht-vor-werbung-unserioeser-online-shops/.

[1268] Google, How Search Works: Crawling, Indexing, and Ranking, available at: https://www.google.com/search/howsearchworks/; Bing Systemic Risk Assessment and Safety Framework Report (2025), p. 23, available at: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/digitalsafety/August-2025-Microsoft-Bing-Systemic-Risk-Assessment-Report-EU-Digital-Services-Act.pdf.

manipulate this pipeline through Search Engine Optimization (SEO) abuse: high keyword density to feign relevance, link farms and 'content spinning' to mimic quality sites, 'typosquatting' or URL hijacking on misspelled brand domains, and selective indexing or 'website cloaking' and 'doorway pages' that present one version of a site to the crawler and another to users.[1269]

A related technique, 'SEO poisoning', is used by criminals to push malware- or scam-hosting pages high in the rankings.[1270] Because ranking confers perceived authority, a high placement, even a temporary one, can divert substantial traffic to illegitimate destinations before detection, and infringers often re-post 'mirror' sites immediately after a URL is demoted or de-indexed.[1271] Search engines themselves actually facilitate this manipulation of search results.[1272] In fact, a recent longitudinal study revealed that Google Search results have become roughly 10% less accurate than in previous years.[1273] Additionally, the study highlighted a growing shift toward repetitive, simplified, and likely AI-generated material.[1274] Google's own Search spam policies state that it uses automated systems to identify and suppress 'imposter sites' and pages that attract users 'on false pretenses'.[1275] Similarly, Bing states that it 'invests significant time and resources to ensure that users are provided with high quality content to avoid the possibility of its page crawlers and algorithms inadvertently returning results that could negatively impact consumers, such as spam or other fraudulent websites.'[1276] However, researchers have found that the improvements cited above have a temporary effect, with SEO manipulators finding new ways to bypass the systems.[1277]

Operational tools and behavioural models relevant to the scam

Fake webshop operators typically register large numbers of domains, often using privacy-protection services to obscure registrant identity. These domains frequently mimic legitimate brand names through typosquatting or incorporate generic product-related terms. The operators use automated tools to rapidly deploy templated websites across multiple domains, creating a distributed infrastructure that is resilient to individual

[1269] Makoto Shimamura, Uncovering Black-hat SEO based fake E-commerce scam groups from their redirectors and websites (2025), available at: https://arxiv.org/html/2505.21021v1

[1270] ibid.

[1271] ibid.

[1272] Janek Bevendorff et al., Is Google Getting Worse? A Longitudinal Investigation of SEO Spam in Search Engines (2024), available at: https://downloads.webis.de/publications/papers/bevendorff_2024a.pdf.

[1273] ibid.

[1274] ibid.

[1275] Google Search Central, Spam policies for Google web search, available at: https://developers.google.com/search/docs/essentials/spam-policies. New Jersey Cybersecurity & Communications Integration Cell, Beware of SEO Poisoning and Malvertising (2023), available at: https://www.cyber.nj.gov/Home/Components/News/News/225/.

[1276] Bing Systemic Risk Assessment and Safety Framework Report (2025), p. 64, available at: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/digitalsafety/August-2025-Microsoft-Bing-Systemic-Risk-Assessment-Report-EU-Digital-Services-Act.pdf.

[1277] Janek Bevendorff et al., Is Google Getting Worse? A Longitudinal Investigation of SEO Spam in Search Engines (2024), available at: https://downloads.webis.de/publications/papers/bevendorff_2024a.pdf.

takedowns.[1278] In this context, Watchlist Internet notes that criminals copy the websites of legitimate online shops so convincingly that the forgery is not apparent at first glance, and that these fake shops are then made 'quickly findable' through well-chosen domain names or paid advertising, in some cases appearing as the first search result when a consumer searches for a specific product.[1279]

Additionally, this type of scam consistently relies on commercial website builders and infrastructure providers. Specifically, platforms like Shopify are used to create professional-looking storefronts, while services like Cloudflare are leveraged to hide the true hosting origins.[1280] These tools allow scammers to scale their operations, semi-automatically building large numbers of near-identical e-commerce sites with customised names, logos and quality-assurance procedures so that they appear legitimate.[1281] The operation deliberately favoured previously expired domains that carried a good Google Search reputation, and its orchestration capabilities let it deploy new webshops or rotate payment pages and domains within hours in response to takedowns.

EUIPO identifies two additional tactics as forms of ranking abuse: The first is 'expired domain abuse' where an individual purchases and repurposes an expired domain to inherit the previous site's ranking and perceived legitimacy. The second is the use of 'mirror' sites, which involves reposting the same content immediately after the original URL has been de-indexed or demoted.[1282]

Furthermore, the emergence of generative AI tools has significantly lowered the barriers to creating convincing fake webshops. Operators use AI to generate product descriptions, customer reviews, legal pages (terms and conditions, privacy policies, return policies), and other content that lends an appearance of legitimacy. AI-powered translation tools enable operators to create localised versions of fraudulent sites targeting multiple language markets simultaneously.[1283] By leveraging AI to generate text, mimic brand visuals, and create realistic product listings, bad actors have significantly reduced the time and expense required to build convincing fake online stores.[1284]

There are several ways in which AI and automated tools are exploited to produce content that manipulates search engine indexation and ranking. 'Content spinning' (also referred

[1278] Europol, Internet Organised Crime Threat Assessment (IOCTA) (2023), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/IOCTA%202023%20-%20EN.pdf.

[1279] Watchlist Internet, "Wege in Fake-Shops" (Paths into Fake Shops), available at: https://www.watchlist-internet.at/news/wege-in-fake-shops/.

[1280] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[1281] Platon Kotzias et al., Scamdog Millionaire: Detecting E-commerce Scams in the Wild (2023), available at: https://dl.acm.org/doi/pdf/10.1145/3627106.3627184.

[1282] EUIPO, Search Engines – Challenges and Good Practices to Limit Search Traffic (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf.

[1283] OECD, Illicit Trade: Converging Criminal Networks (2022), available at: https://books.google.be/books/about/Illicit_Trade.html?id=g8MFkAEACAAJ&redir_esc=y.

[1284] Survey among national authorities on Scoping of the National Online Fraud Landscape in the EU Member States under the DSA.

to as ‘website spinning’ or ‘article spinning’) is a technique by which operators use automated means to rewrite text from existing, legitimate websites, producing multiple near-unique versions of the same content so that each version appears to the search engine's crawler as original, thereby evading duplicate-content filters and improving the ranking of the fraudulent site.[1285] It is used to create an impression of licit quality content, in effect allowing a fake or infringing site to mimic the appearance of a legitimate, high-quality website in the eyes of both the ranking algorithm and the end user.[1286] The same technique is used at the site level to produce ‘mirror’ websites that share the same infringing or fraudulent content but differ slightly in presentation, making it harder for rights holders and search engines to detect and act on the copies, and allowing rapid reposting after a takedown.[1287] On the advertising side, it is observed that AI is already being used by search engines to generate ‘personalised ads and descriptions of content on the spot, based on user query and other factors,’ citing Google's own announcement of ‘a new era of AI-powered ads.’[1288]

Consumer-protection bodies across Europe have cautioned that AI makes it increasingly difficult for consumers to distinguish real shops from fake ones, as the quality of fraudulent content now approaches that of legitimate commercial websites.[1289] Watchlist Internet’s operational experience confirms this at the ground level: it observes that well-made fake shops ‘steal the company data of reputable sites’ and replicate the genuine website so convincingly that the forgery is often not apparent at first glance, and that criminals now use these copied sites together with Google Ads to ensure they appear prominently to consumers.[1290]

The success of fake webshops also depends on exploiting cognitive biases and behavioural patterns. Fake webshop scams primarily exploit consumer psychology by offering unrealistically low prices.[1291] Fraudsters enhance this tactic by creating artificial scarcity and urgency through heavy discounts (often up to 80%), limited stock alerts, and countdowns like 'sale ends today'.[1292] Consumer authorities corroborate this pattern: guidance from the ECC-Net treats unrealistically low prices that are inconsistent with other sites as a warning sign, often paired with claims that only a few minutes or a few items remain, together with countdown timers and limited-stock claims as core pressure

[1285] Nowspeed, What is Article Spinning and Why Is It "Black Hat" SEO?, available at: https://nowspeed.com/blog/bad-seo-content-spinning/.

[1286] ibid.

[1287] ibid.

[1288] Google Ads and Commerce Blog, Introducing a new era of AI-powered ads with Google (2023), available at: https://blog.google/products/ads-commerce/ai-powered-ads-google-marketing-live/.

[1289] European Consumer Centre (ECC-Net), Online Shopping and Consumer Rights (2023), available at: https://commission.europa.eu/topics/consumers/consumer-rights-and-complaints/resolve-your-consumer-complaint/european-consumer-centres-network-ecc-net_en.

[1290] Watchlist Internet, Das können Sie tun, wenn Kriminelle Ihren Online-Shop kopieren, available at: https://www.watchlist-internet.at/news/das-koennen-sie-tun-wenn-kriminelle-ihren-online-shop-kopieren/.

[1291] Competition and Consumer Protection Commission (CPCC), Scams – Real cases, real consequences: A collection of case studies and lessons for consumers (2025), available at: https://www.ccpc.ie/consumers/wp-content/uploads/sites/2/2025/11/Scams-Real-cases-real-consequences-CCPC.pdf.

[1292] ibid.

tactics.[1293] These high-pressure tactics exploit consumer price sensitivity and time anxiety, effectively bypassing the victim's scepticism. Scammers strategically align their operations with peak retail seasons; consequently, the weeks surrounding Black Friday, pre-Christmas shopping, and post-Holiday returns see a sharp spike in fraudulent webshop reports.[1294]

Service-level interventions

Neither Google's, nor Bing's 2025 SRA uses the specific term 'fake webshop advertisements' as a distinct category. [1295] Both reports instead address the broader phenomena of fraudulent, deceptive, and scam-related advertising and commercial practices on search engines, within which fake webshop advertisements would fall, and the following analysis draws on those findings. Bing, for its part, expressly frames 'Consumer Protection and Fraud' to include exposure to scams, spam, false representation, fraudulent businesses, and deceptive commercial practices, rating the inherent risk as 'High' (inherent probability 'Likely,' inherent severity 'High') before mitigations, and 'Low' on a residual basis once its mitigations are applied.[1296] Google's SRA addresses the phenomenon under the 'Consumer and Business' dimension of its systemic risk assessment, which includes two risk statements: the 'risk that unfair commercial practices take place on a service' and the 'risk that misrepresentation or misleading information about a business is available on a service.'[1297] In the Search-specific section of its report, Google discusses these risks under the heading 'Addressing Unfair Commercial Practices and Fraudulent Content about a Business'.[1298]

Both Google Search and Microsoft Bing indicated that they have developed multi-layered platform-level interventions to combat fraudulent and deceptive advertising and commercial practices on their search engines, which encompass the type of harm posed by fake webshop advertisements.[1299]

Google Search reports that investments in its AI-powered scam detection systems have enabled it to detect twenty times the number of 'scammy' pages compared to prior periods, and that AI tools help detect and block hundreds of millions of fraudulent search results daily.[1300] In 2024, Google blocked or removed 415 million ads and suspended over 5 million accounts for violating ads policies most closely associated with scams.[1301]

[1293] European Consumer Centres Network, 5 Tips for Safe Shopping on Black Friday (2022), available at: https://www.eccnet.eu/news/5-tips-safe-shopping-black-friday.

[1294] Survey among national authorities on "Scoping of the National Online Fraud Landscape in the EU Member States under the DSA".

[1295] Google, Bing 2025 Systemic Risk Assessment Reports.

[1296] Bing 2025 Systemic Risk Assessment Report.

[1297] Google 2025 Systemic Risk Assessment Report.

[1298] ibid.

[1299] Google, Bing 2025 Systemic Risk Assessment Reports.

[1300] Google 2025 Systemic Risk Assessment Report.

[1301] ibid.

On the Bing side, it is indicated that Microsoft Advertising enforces content policies that prohibit misleading, deceptive, and fraudulent advertisement content, complemented by Relevance and Quality Policies and a combination of human and automated review covering ad text, images, product feeds, landing pages, URLs, keywords, and targeting settings.[1302] It employs a multi-tiered fraud detection system built on machine-learning models, heuristic sweeps/rules, and manual reviews.[1303] This includes advertiser-level models such as payment fraud detection, a behavioural risk model that assesses account and campaign features to gauge whether an advertiser is fraudulent, and LLM-based spoofing detection, which specifically targets advertisers pretending to be a legitimate site (for example, deceiving users into believing an ad leads to the official website of a bank).[1304] Bing also reports that it operates Advertiser Identity Verification (AIV), which requires advertisers to prove their legal identity before they can run ads and acts as a deterrent to bad actors engaged in phishing scams, personal-information fraud, and the advertising of disallowed products.[1305]

Furthermore, both search engines indicate that they implement anti-scam defences in their indexing and ranking systems.

Google states that Search employs advanced AI technologies to detect and block hundreds of millions of fraudulent results daily, significantly enhancing its ability to identify and remove scam pages from organic results.[1306] Google Search claims its ranking approach surfaces credible, high-quality content over lower-quality content, and it has strengthened its spam policies to act against the use of automation to generate low-quality or unoriginal content at scale with the goal of manipulating search rankings, including pages that pretend to answer popular searches but fail to deliver helpful content.[1307] Its Search Quality Rating Program, using external quality raters, is meant to evaluate whether Search systems generate results that demonstrate experience, expertise, quality, and trustworthiness.[1308]

Bing similarly describes its ranking algorithms as ‘the first and strongest defence’ in delivering safe, authoritative content: they are designed to prevent users from being exposed to low-quality content, including websites engaging in scams or fraudulent activities, elevating trusted sources and reducing the visibility of unreliable or manipulated content rather than removing it outright.[1309] Bing claims it uses a Quality and Credibility (‘QC’) score incorporating external signals to elevate trusted results and demote pages that may be misleading or exploitative, and that its ranking systems are explicitly designed to defend against manipulation, including spam and search engine optimisation abuse.[1310] Its Webmaster Guidelines prohibit practices intended to

[1302] Bing 2025 Systemic Risk Assessment Report.

[1303] ibid.

[1304] ibid.

[1305] ibid.

[1306] Google 2025 Systemic Risk Assessment Report.

[1307] ibid.

[1308] ibid.

[1309] Bing 2025 Systemic Risk Assessment Report.

[1310] ibid.

manipulate or deceive the Bing Search algorithms (such as keyword stuffing and other spam and fraud tactics) and a dedicated Webmaster team monitors and addresses abusive SEO techniques.[1311] Bing additionally reports that it leverages external signals to assess whether a particular advertiser or domain poses a risk to consumers, including signals from VirusTotal (an aggregator of malware risk signals), domain tools that indicate domain risk, and 'Who is' data providing the age and expiry of a domain and click-through data on Bing and Google Search.[1312]

Limitations of current measures and systemic challenges identified

Despite the interventions described above, both search engine providers acknowledge persistent systemic challenges in combating fraudulent and deceptive commercial practices, including fake webshop advertisements, on their services.

Google's report explicitly recognises that risk from highly motivated bad actors continues to be of concern in connection with threats such as fraud, scams, and malware, noting the wider availability of increasingly sophisticated technology, the determined nature of these actors, and the importance of industry-wide and multi-stakeholder efforts to address the challenges.[1313] Google further notes that scams are increasing in both volume and complexity, are often carried out by bad actors who operate at scale, constantly adapt their methods, and combine online and offline activity to lure people into fraudulent schemes.[1314] The rapidly expanding accessibility of AI tools has allowed bad actors to develop new efficiencies in existing fraud and abuse vectors, leveraging transformer-based large language models, text-to-image, and video and audio generators to scale traditional scams by exploiting existing vulnerabilities more efficiently.[1315]

On the indexing and ranking dimension of this case study, Google identifies a structural limitation inherent to how Search works: because Search indexes the open web, 'some degree of manageable risk associated with potentially illegal or 'legal but harmful' content will always be present within Search results, simply because open web content may still be discoverable if it is available on the internet'.[1316] Content that Search has no legal obligation to remove and that is not prohibited by its policies remains available in search results for users who express an intent to explore it, even where indicators suggest it is of relatively low quality or potentially harmful, and Google states that this continued availability results in elevated levels of residual risk.[1317] Google Search claims that its chosen approach is to raise the ranking of the highest-quality information rather than to remove low-quality information, an emphasis on ranking rather than availability that it considers proportionate but that necessarily leaves fraudulent content discoverable.[1318]

[1311] Bing, Bing Webmaster Guidelines, available at: https://www.bing.com/webmasters/help/webmaster-guidelines-30fba23a.

[1312] Bing 2025 Systemic Risk Assessment Report.

[1313] Google 2025 Systemic Risk Assessment Report.

[1314] ibid.

[1315] ibid.

[1316] ibid.

[1317] ibid.

[1318] ibid.

Applied specifically to fraudulent commercial content, Google Search acknowledges that although it prioritises the highest-quality results in ranking and removes fraudulent content subject to valid legal removal requests, such content 'will continue to be returned in search results when a user seeks it out,' provided it is not the subject of a valid legal removal request or prohibited by Google policies and is still available on the internet, so that some residual risk of fraudulent business information appearing on Search remains.[1319]

On the Bing side, while Microsoft assessed the residual risk for Consumer Protection and Fraud as "Low," it is further noted that the risk landscape is dynamic: spam tactics are often used by bad actors to manipulate ranking and show up in search results, and Bing must continuously monitor manipulation trends in high-risk areas and deploy mitigations to ensure quality results are returned.[1320] A fundamental structural limitation identified by Bing, relevant to indexing and ranking, is that the primary content appearing on Bing is information from third-party websites: webmasters are not users of Bing and Bing has no contractual privity with them, meaning Bing has limited ability to enforce rules regarding content appearing on those third-party sites and instead focuses on ranking and targeted filtering rather than removal.[1321]

EUIPO reinforces this convergence from the intellectual-property enforcement perspective. It stresses that 'de-indexing' a page from a search engine does not remove it from the web, and that users continue to access content in other ways.[1322] It also documented that ranking interventions are frequently only temporary, because website owners change their SEO strategy again after being demoted or de-indexed, and repost 'mirror' sites immediately after action is taken.[1323]

For paid results, it also observes that, given the sheer number of advertisers and the largely automated advertising process, it is difficult for search engines to control the 'quality' of advertisers on a case-by-case basis or to continuously identify when a paid advertisement is actually linked to fraudulent content.[1324] Both systemic risk assessment reports thus converge on a key systemic challenge: search engines can demote, delist, or refuse to advertise fraudulent content, but they cannot remove it from the web, and the arms race between platform mitigations and increasingly sophisticated bad actors,

[1319] ibid.

[1320] Bing 2025 Systemic Risk Assessment Report.

[1321] ibid.

[1322] EUIPO, Search Engines – Challenges and Good Practices to Limit Search Traffic (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf; TorrentFreak, Share With Care: 2,217 Domains Blocked, The Majority For Circumvention (2024), available at: https://torrentfreak.com/share-with-care-2217-pirate-domains-blocked-most-for-circumventing-blocking-240114/.

[1323] Janek Bevendorff et al., Is Google Getting Worse? A Longitudinal Investigation of SEO Spam in Search Engines (2024), available at: https://downloads.webis.de/publications/papers/bevendorff_2024a.pdf.

[1324] TorrentFreak, Google Sees DMCA Takedown Requests Surge to New Highs (2024), available at: https://torrentfreak.com/google-sees-dmca-takedown-requests-surge-to-new-highs-240110/; TorrentFreak, Google Search Processed a Billion DMCA Takedowns in Four Months (2024), available at: https://torrentfreak.com/google-search-processed-a-billion-dmca-takedowns-in-four-months-240622/; TorrentFreak, Google Asked to Remove 10 Billion "Pirate" Search Results (2024), available at: https://torrentfreak.com/google-asked-to-remove-10-billion-pirate-search-results-241105/.

amplified by generative AI, ensures that some level of residual risk from fake and fraudulent commercial content, including fake webshop advertisements, persists.[1325]

Conclusions and recommendations

This case study finds that fake webshops reach consumers through a chain of search engine design features. Paid advertising sold through keyword auctions, ad placement at the top of the results page, and organic indexing and ranking each supply illegitimate sellers with the visibility and apparent credibility of legitimate ones. Operators exploit this chain with SEM techniques (bidding on brand keywords, deceptive ads impersonating an 'official web store,' and ad cloaking) and SEO techniques (keyword stuffing, content spinning, typosquatting, website cloaking, doorway pages, and expired-domain abuse). These techniques are industrialised through commercial infrastructure and franchised 'infrastructure-as-a-service' operations, accelerated by generative AI, and monetised by exploiting price sensitivity, urgency cues, and seasonal shopping peaks.

Against that backdrop, the EUIPO report holds that robust 'Know Your Business Customer' (KYBC) verification, requiring advertisers to disclose and prove identity, business operation, source, location, and, where relevant, proof of authenticity before running ads, could increase accountability and improve detection of bad actors.[1326] Terms and conditions that prohibit fraudulent and IP-infringing advertising and enforce repeat-infringer policies through warnings, ad removal, and account suspension or termination are also identified by EUIPO as relevant countermeasures.[1327]

Similarly, BEUC calls for trader traceability processes that hinder rogue traders from 're-spawning' under new accounts.[1328] At public level, Austrian bodies maintain practical consumer-protection infrastructure: the Watchlist Internet platform publishes lists of fraudulent online shops, and the associated 'Fake-Shop Detector' browser tool, developed by ÖIAT and AIT, warns users in real time against known or AI-flagged fraudulent shops.[1329]

[1325] Google, Systemic Risk Assessments Report (2025), available at: https://storage.googleapis.com/transparencyreport/report-downloads/dsa-risk-assessment_2025-8-28_2025-8-28_en_v1.pdf; Bing, Systemic Risk Assessment Report (2025), available at: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/digitalsafety/August-2025-Microsoft-Bing-Systemic-Risk-Assessment-Report-EU-Digital-Services-Act.pdf.

[1326] EUIPO, Search Engines – Challenges and Good Practices to Limit Search Traffic (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf.

[1327] ibid.

[1328] BEUC, DSA trilogue recommendations and press statement, incl. TechCrunch coverage (2022), available at: https://techcrunch.com/2022/04/13/dsa-beuc/; BEUC, Digital Services Act should help consumers online but success depends on strong enforcement (2022), available at: https://www.beuc.eu/press-releases/digital-services-act-should-help-consumers-online-success-depends-strong-enforcement.

[1329] Watchlist Internet, "Liste betrügerischer Online-Shops," available at: https://www.watchlist-internet.at/liste-betruegerischer-shops/; ÖIAT/AIT, Fake-Shop Detector, available at: https://research.oiat.at/fake-shop-detector.

In relation to paid search results, EUIPO refers to automated ad-review tools, AI-assisted checks to catch cloaked ads that swap content after approval and guided and bulk notification mechanisms as relevant countermeasures.[1330]

For organic results, the EUIPO refers to the demotion or de-indexation of sites that engage in scam or spam behaviour as a potential avenue for action, suggesting that expired-domain abuse and scaled machine-generated content could qualify as spam.[1331] Automated spam- and malware-detection tools (for example against typosquatting) and adapting ranking algorithms are also listed as relevant countermeasures, in addition to measures blocking infringement- and scam-related terms from autocomplete.[1332] The EUIPO research also explores the use of automatically generated information panels to steer users toward official or authoritative sources.[1333] Finally, the agency lists guided and bulk notice-and-action channels, trusted-flagger schemes that prioritise notifications from parties with a proven track record, 'not-yet-indexed' URL reporting, and the publication of transparency reports on actions taken, complemented by awareness campaigns and warning messages, as measures of relevance in a strategy to combat online financial scams on search engines.[1334]

The case study finds that fake webshops operate at the level of visibility rather than existence. Because search engines cannot remove content from the web and bad actors continuously adapt, fake webshop exposure is best treated as a residual risk to be continuously managed through layered platform mitigations, cross-industry cooperation, and consumer awareness.

6.4. Case study D: Health and wellness scams on e-commerce platforms

Purpose of the case study

Health and wellness scams, encompassing the fraudulent promotion of ineffective or non-existent medical treatments, dietary supplements, weight loss products, cosmetic procedures, and health monitoring devices, represent one of the most pervasive and harmful categories of online scams. Health and wellness scams operate at the intersection of financial scams and public health harm, actively relying on misinformation as a propagation vector. The alignment between the structure of product listings, consumer demand for health-related goods, and the primary target profile of health and wellness scams on e-commerce platforms reflects deliberate targeting decisions by scammers. This topic has been chosen as it allows an in-depth exploration of the increase in health conspiracies and financial scams.

[1330] EUIPO, Search Engines – Challenges and Good Practices to Limit Search Traffic (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf.

[1331] ibid.

[1332] ibid.

[1333] ibid.

[1334] ibid.

Scope and methodology

This case study prioritises e-commerce marketplaces that intermediate the sale of physical goods and health-related products. It examines how marketplace design, seller onboarding and traceability, listing and advertising systems, recommender algorithms, review and rating mechanisms, and fulfilment/logistics services shape both exposure to and mitigation of health and wellness scams. The case study considers the services provided by AliExpress, Amazon Store, Google Shopping, Shein, Temu and Zalando as part of the scope.

Methodologically, the study triangulates (i) DSA materials, including VLOP/VLOSE risk reports, enforcement actions, the DSA Transparency Database and related Commission and CPC Network activity; (ii) regulatory and enforcement materials from medicines, consumer-protection, product-safety, customs, and law-enforcement authorities, including EMA/HMA, Europol, INTERPOL, FDA, and EU online-pharmacy materials; (iii) consumer and civil-society evidence, including BEUC materials, national consumer-organisation findings, and trusted flagger research; (iv) academic literature and investigative reporting on online health fraud; (v) targeted interview data from Tasks 1 and 2; (vi) the case study findings as explored and validated through the workshop (Task 4).

Background on scam model, prevalence and impact

Health and wellness scams refer to the online marketing and sale of unregulated medicines, medical devices or procedures, cosmetics or wellness products, based on false or misleading claims. Under this category, scammers promote and sell illegal counterfeit medicines, or other harmful and/or unregulated health products or services.[1335] The marketing of these products is perpetrated by criminal networks with flexible structures, which may also engage technical experts or legal and financial advisors to facilitate their processes, as reported by Europol.[1336] The scale of these criminal networks has been further confirmed by INTERPOL's Operation Pangea XVII (December 2024–May 2025), which resulted in 769 arrests, the dismantling of 123 criminal groups across 90 countries, and the seizure of 50.4 million doses of illicit pharmaceuticals worth USD 65 million (approx. EUR 56 million).[1337]

The main categories of medical products that are diverted and misused throughout the EU as a result of health and wellness scams are: anticonvulsant or antiepileptic drugs, synthetic opioids, anti-cancer drugs, erectile dysfunction medicines, pseudoephedrine, doping substances, painkillers, antioestrogens, antivirals, hypnotics, antihistamines, anxiolytics, appetite suppressors (semaglutide), diabetes pens, or performance-

[1335] Health Products Regulatory Authority (HPRA), Urgent warning of fraudulent websites and adverts promoting illegal medicines (2025), available at: https://www.hpra.ie/news-events/news/article/urgent-warning-of-fraudulent-websites-and-adverts-promoting-illegal-medicines.

[1336] Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/The_threat_of_pharmaceutical_crime_in_the_EU_and_beyond.pdf.

[1337] Interpol, Record 769 arrests and USD 65 million in illicit pharmaceuticals seized in global bust (2025), available at: https://www.interpol.int/en/News-and-Events/News/2025/Record-769-arrests-and-USD-65-million-in-illicit-pharmaceuticals-seized-in-global-bust.

enhancing drugs.[1338] The proliferation of counterfeit semaglutide-based products (marketed as GLP-1 analogues for weight loss) has become a particularly acute concern; Europol Operation SHIELD VI (April–November 2025) specifically highlighted the 'proliferation of counterfeit Semaglutide-based products used as fat-burners' as a critical public health threat, resulting in 3,354 prosecutions, 907 investigations, and 43 organised crime groups investigated across 30 countries.[1339]

This trend reflects an increasing reliance on self-medication among the general population, which poses important threats to public health. As these falsified or counterfeit health and wellness products are often produced in underground laboratories, without safety measures in place, consumers are exposed to severe risks, including treatment failure, toxicity or even death.[1340] Beyond the biological risks associated with these products, victims also suffer from financial loss and psychological harms, as they may experience anxiety over the effects of taking substandard medications.[1341] At an aggregated level, health and wellness scams are a public health threat, as they may increase the general burden of illness on a society.[1342] The OECD and EUIPO have estimated that the global trade in counterfeit goods (in general) reached approximately USD 467 billion (approx. EUR 408 billion) in 2021, representing 2.3% of global trade, with counterfeit pharmaceuticals constituting a significant and growing subset of this illicit economy.[1343]

The financial impact of fake medicines offered online ranks highly – for example, in 2024, the coordinated efforts under Operation SHIELD V (led by Europol) single-handedly led to the seizure of fake medicinal products worth above EUR 11.1 million.[1344]

Examples of health scams have been reported upon by some non-EU authorities. For example, the U.S. Food and Drug Administration (FDA) purchased and tested weight loss and sexual enhancement supplements sold on Amazon and eBay.[1345] The agency found that the products contained a variety of potentially dangerous drugs, which could

[1338] Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/The_threat_of_pharmaceutical_crime_in_the_EU_and_beyond.pdf.

[1339] Europol, Operation Shield (2025), available at: https://www.europol.europa.eu/how-we-work/operations/operation-shield.

[1340] Aonghus J Feeney et al., Global perspective of the risks of falsified and counterfeit medicines: A critical review of the literature (2024), available at: https://www.sciencedirect.com/science/article/pii/S1477893924000759.

[1341] Ankit Raj et al., Counterfeit medicine: a major public health concern and effective remedies for combatting the crisis (2025), available at: https://link.springer.com/article/10.1007/s44395-025-00004-6.

[1342] ibid.

[1343] OECD, Mapping Global Trade in Fakes 2025 (2025), available at: https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en.html.

[1344] Europol, Europol warns consumers to be mindful about fake medicines offered online (2025), available at: https://www.europol.europa.eu/media-press/newsroom/news/europol-warns-consumers-to-be-mindful-about-fake-medicines-offered-online.

[1345] Ryan Felton, FDA Finds Hidden Drugs in Nearly 50 Dietary Supplements Sold on Amazon, eBay (2020), available at: https://www.consumerreports.org/health/fda-finds-hidden-drugs-in-weight-loss-sexual-enhancement-dietary-supplements-sold-on-amazon-ebay-a6199440119/.

cause serious side effects or interact with medications or supplements a consumer is already taking. Several of these fraudulent products, purchased on Amazon, were highlighted as '#1 Best Seller' or 'Amazon's Choice', as per the FDA's findings. The Amazon's Choice badge is given to 'highly rated, well-priced products available to ship immediately', the company informs shoppers throughout its website.[1346]

Relevance to EU citizens and regulatory priorities

EMA and the Heads of Medicines Agencies (HMA) are warning the public about the growing threat of illegal medicines being advertised and sold online across the EU. In September 2025, the EMA flagged a 'sharp rise in illegal medicines marketed as weight-loss and diabetes medicines online,' warning that authorities had identified 'hundreds of fake Facebook profiles, advertisements and e-commerce listings, many of which are hosted outside the EU.'[1347] For EU consumers, e-commerce marketplaces have become a point of exposure to counterfeit and unsafe health products, misleading supplement claims, and fraudulent medical devices. The relevance for EU citizens is further underscored by studies conducted by European and national consumer organisations, which, in assessing the safety of products offered on e-commerce marketplaces such as Temu, AliExpress, and Amazon, have identified unsafe products, including cosmetics and fraudulent health products.[1348]

The scale of the counterfeit health product problem is underscored by INTERPOL's findings, based on analysis of over a decade of Operation Pangea results, that at least 11 per cent of medical products sold online are counterfeit, with all regions of the world affected. While this figure encompasses online sales channels broadly, e-commerce marketplaces represent a significant share of the distribution infrastructure exploited for the trade in counterfeit health products.[1349]

To help the public identify legitimate online medicine retailers, the EU introduced a common logo which appears on the websites of all registered online pharmacies and retailers. Clicking on the logo takes buyers to a national register of authorised

[1346] US Food and Drug Administration , Warning Letter (2024), available at: https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/amazoncom-inc-679523-07252024.

[1347] Reuters, EU regulator flags surge in online sales of counterfeit weight-loss drugs (2025), available at: https://www.reuters.com/sustainability/boards-policy-regulation/eu-regulator-flags-surge-online-sales-counterfeit-weight-loss-drugs-2025-09-03/; European Medicines Agency, Warning about sharp rise in illegal medicines sold in the EU (2025), available at: https://www.ema.europa.eu/en/news/warning-about-sharp-rise-illegal-medicines-sold-eu.

[1348] See for example BEUC, Under the Microscope: Tests of Temu Products by Consumer Groups (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-007_Tests_of_Temu_Products_by_Consumer_Groups.pdf; BEUC, Unsafe and Illegal Activities Online, available at: https://www.beuc.eu/sites/default/files/publications/unsafe_and_illegal_activities_online.pdf; BEUC, Sponsored by Scammers (2026), available at: https://www.beuc.eu/reports/sponsored-scammers; Stiftung Warentest, Gefährliche Schnäppchen (2025), available at: https://www.test.de/Temu-und-Shein-Gefaehrliche-Schnaeppchen-6253491-0/.

[1349] Interpol, Operation Pangea – shining a light on pharmaceutical crime (2019), available at: https://www.interpol.int/News-and-Events/News/2019/Operation-Pangea-shining-a-light-on-pharmaceutical-crime.

retailers.[1350] If a website does not have this logo or is not listed on a national register, the website is fraudulent and operates illegally. The national flag and the text are an integral part of the logo. Only national flags of an EU Member State, as well as those of Norway, Iceland and Liechtenstein, can be displayed.

At platform-level, the DSA imposes risk-management, trader traceability, notice-and-action, and transparency duties on large intermediaries, while the General Product Safety Regulation (EU) 2023/988 strengthens market surveillance and recalls. Together, these frameworks make online marketplace governance a public-law priority given the direct health and economic harms documented by EU and national authorities.

Description of platform features relevant to scam propagation

E-commerce platforms designated as VLOPs exhibit a range of structural features that can facilitate the propagation of health and wellness scams. These features span the full user journey: from product discovery – shaped by algorithmic recommendation, search ranking, and sponsored placements – to trust formation via ratings, reviews, and seller verification signals, to transaction completion through integrated payment and fulfilment systems.[1351]

The scale, speed, and cross-border reach of these platforms create an environment in which fraudulent health products – including ineffective dietary supplements, counterfeit pharmaceuticals, unproven medical devices, and fabricated wellness treatments – can be listed, promoted, purchased, and shipped before effective enforcement action can be taken.[1352] Furthermore, the marketplace model, in which platforms host large volumes of third-party sellers, introduces layers of complexity for trader verification, content moderation, and regulatory compliance.

On marketplaces, as documented in enforcement analyses by Europol and EUIPO, the key risk drivers include:

(a) large volumes of third-party sellers, including extra-EU traders;
(b) rapid, low-friction listing creation with limited pre-verification of health claims;
(c) search and sponsored-listing placements that can surface non-compliant products;
(d) algorithmic ranking systems that concentrate demand;
(e) seller use of fulfilment services that lend perceived legitimacy; and
(f) manipulation of ratings, reviews and Q&A to simulate efficacy and safety.[1353]

[1350] European Medicines Agency, Buying medicines online, available at: https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview/buying-medicines-online.

[1351] OECD/EUIPO, Misuse of E-Commerce for Trade in Counterfeits (2021), available at: https://www.oecd.org/en/publications/misuse-of-e-commerce-for-trade-in-counterfeits_1c04a64e-en.html; Europol-EUIPO, Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact (2024), available at: https://www.euipo.europa.eu/en/publications/uncovering-the-ecosystem-of-intellectual-property-crime-a-focus-on-enablers-and-impact.

[1352] Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/publications-events/publications/threat-of-pharmaceutical-crime-in-eu-and-beyond; Interpol, Operation Pangea – shining a light on pharmaceutical crime (2019), available at: https://www.interpol.int/en/News-and-Events/News/2019/Operation-Pangea-shining-a-light-on-pharmaceutical-crime.

[1353] ibid.

Among the most pertinent risk vectors, algorithmic personalisation systems tailor content based on users' browsing history and thereby enable scammers to target individuals with health-related scams customised to their interests. For example, research on older adults' vulnerability to health scams has identified such personalisation mechanisms as a key factor in channelling potential victims toward fraudulent health product listings. The same study found that e-commerce platforms' integrated payment and dispute resolution systems offer consumers a degree of protection against health fraud, concluding that online payment and shopping features did not significantly increase health scam exposure among older users – attributing this in part to defensive mechanisms embedded in e-commerce platforms, such as customer service support and dispute resolution services. Nonetheless, the speed and volume of transactions on large marketplaces can still create opportunities for fraudulent sellers to process payments before platform-level safeguards are triggered.[1354]

The structured nature of the criminal organisations behind these scams can also be observed when comparing the content of these fraudulent ads across different EU Member States – often, they are just different translations of the same post, or follow a very similar structure and phrasing.[1355] These fraudulent ads lead to cloned websites or fake webshops, through which users are prompted to buy the products. In the e-commerce context, these fake webshops frequently mimic the appearance of legitimate marketplace storefronts, and criminal networks may operate through third-party seller accounts on established platforms to exploit the trust and reach associated with those platforms. Cybercriminals can exploit online e-commerce platforms by creating counterfeit retail webpages, advertising or selling fake healthcare products, and stealing financial information during transactions. [1356]

Influencer endorsements are also sometimes used to promote these fraudulent products.[1357] While influencer activity primarily occurs on social media platforms, its relevance to e-commerce is direct: influencers frequently link to marketplace product listings or seller storefronts, and their endorsements may be repurposed in product descriptions, reviews, or advertising on e-commerce platforms, thereby driving consumer traffic toward fraudulent health products. It is unclear whether the influencers promoting these health or wellness scam products are aware of their fraudulent nature. Nonetheless, they represent a very important actor in the propagation of these scams – for example, as reported by Europol, dietary and nutrition influencers have become the main marketing power behind the marketing and sale of illicit hormonal substances.[1358]

[1354] Hongliang Chen, et al., Examining older adults' vulnerability to online health scams: insights from routine activity theory (2025), available at: https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2025.1585851/full.

[1355] ibid.

[1356] ibid.

[1357] David Sheperd et al., The Impact of Deviant Social Media Influencers and Consumer Characteristics on Purchasing Counterfeit Goods (2023), available at: https://www.tandfonline.com/doi/epdf/10.1080/01639625.2023.2233041?needAccess=true.

[1358] Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/The_threat_of_pharmaceutical_crime_in_the_EU_and_beyond.pdf; Europol-EUIPO, Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact (2024), accessible at: https://www.europol.europa.eu/publications-events/publications/uncovering-ecosystem-of-intellectual-property-crime.

Marketplace design also shapes enforcement frictions. Even with KYBC and trader traceability requirements, OECD and EUIPO report that platforms face persistent difficulty adequately vetting third-party sellers, and efforts to identify and discipline sellers of counterfeit or fraudulent goods must constantly be updated as bad actors adapt.[1359]

Operational tools and behavioural models relevant to the scam

On marketplaces, bad actors can exploit the trust architecture of e-commerce by attaching offers to existing product detail pages, manipulating product variants, relying on sponsored placements, or benefiting from accumulated reviews that do not necessarily correspond to the product ultimately supplied. Consumer Reports has documented how hijacked or merged reviews on Amazon can mislead consumers about the quality and identity of products, and Amazon's own brand-protection materials.[1360] Amazon recognises that infringing content, counterfeits, abuse, and inaccurate product information can appear on product detail pages and listings.[1361]

Scammers usually rely on the misuse of official logos or certifications.[1362] In this context, EMA and HMA have specifically warned that illegal medicines, including GLP-1 products, are promoted through fraudulent websites, advertisements and e-commerce listings, often using official logos and false endorsements.[1363]

In general, dropshipping or shipment from third-country sellers also creates enforcement problems: the Commission's e-commerce toolbox links the growth of third-country e-commerce imports to health and safety risks, while the European Parliament has warned that where non-EU sellers are not traceable or use false addresses, authorities may have no liable legal entity against which to act.[1364]

[1359] OECD/EUIPO, Misuse of E-Commerce for Trade in Counterfeits, Illicit Trade, OECD Publishing (2021), available at: https://doi.org/10.1787/1c04a64e-en.

[1360] Consumer Reports, Hijacked Reviews on Amazon Can Trick Shoppers (2019), available at: https://www.consumerreports.org/customer-reviews-ratings/hijacked-reviews-on-amazon-can-trick-shoppers/.

[1361] Amazon, 'Brand Protection Report' (2024), available at: https://assets.aboutamazon.com/98/b9/fd43272244559ce52b6144103164/amazon-brand-protection-report-2024.pdf.

[1362] European Medicines Agency, Warning about sharp rise in illegal medicines sold in the EU (2025), available at: https://www.ema.europa.eu/en/news/warning-about-sharp-rise-illegal-medicines-sold-eu.

[1363] European Medicines Agency, Warning about sharp rise in illegal medicines sold in the EU (2025), available at: https://www.ema.europa.eu/en/news/warning-about-sharp-rise-illegal-medicines-sold-eu; European Medicines Agency, EU actions to tackle shortages of GLP-1 receptor agonists (2024), available at: https://www.ema.europa.eu/en/news/eu-actions-tackle-shortages-glp-1-receptor-agonists.

[1364] European Parliament, Report on product safety and regulatory compliance in e-commerce and non-EU imports (2025), available at: https://www.europarl.europa.eu/doceo/document/A-10-2025-0133_EN.html; European Commission, E-commerce communication: a comprehensive EU toolbox for safe and sustainable e-commerce (2025), available at: https://digital-strategy.ec.europa.eu/en/library/e-commerce-communication-comprehensive-eu-toolbox-safe-and-sustainable-e-commerce.

Additionally, generative AI is used to generate the content of ads. For example, a report from Check Point highlights the use of dramatic, AI-generated 'before' and 'after' photos used to promote weight loss products or appetite inhibitors (GLP1).[1365]

In terms of behavioural models, health and wellness scams take advantage of the general public's fear of illness, promising 'cures' against diseases most prevalent within the population. This approach was particularly visible during the COVID-19 pandemic, when scammers promoted fraudulent medical products through allegations that these would cure or protect against the virus, and that they were recommended by official health authorities.[1366] A CPC sweep from 2020 found that 30% of the checked websites selling health products contained products with fraudulent claims of healing or preventive effectiveness against the coronavirus.[1367]

Research on the elderly's vulnerability to health scams also finds that exposure to promotional health messaging – whether encountered online or offline – and a heavier chronic disease burden were both significantly associated with greater exposure to health scam content, suggesting that older adults actively managing health conditions are disproportionately targeted with these specific categories of deceptive claims.[1368]

Health and wellness scams do not operate in an informational vacuum; they frequently intersect with health conspiracy theories, which both generate demand for and lend credibility to fraudulent products. Research has identified widespread conspiracy beliefs relating to HIV/AIDS, vaccines, pharmaceutical companies and COVID-19, which are associated with increased mistrust of health authorities and a greater reliance on unproven alternative therapies, driven by factors such as sociopolitical distrust, cognitive biases, low scientific literacy and the widespread dissemination of misinformation online.[1369] This distrust is often commercially exploited. The monetisation of vaccine disinformation has been linked to the sale of dietary supplements and alternative health products by so-called 'conspiratorial wellness influencers',[1370] while Bitdefender Labs notes that declining trust in conventional medicine, exacerbated by pharmaceutical

[1365] Check Point, Inside Europe's AI-Fuelled GLP-1 Scam Epidemic: How Criminal Networks Are Hijacking the Identities of the NHS, AEMPS, ANSM, BfArM and AIFA to Sell Fake Weight-Loss Products (2025), available at: https://blog.checkpoint.com/research/inside-europes-ai-fuelled-glp-1-scam-epidemic-how-criminal-networks-are-hijacking-the-identities-of-the-nhs-aemps-ansm-bfarm-and-aifa-to-sell-fake-weight-loss-products/.

[1366] ACAMS, Fraud and Fear: COVID-19 Scams (2021), available at: https://www.acams.org/en/opinion/fraud-and-fear-covid-19-scams.

[1367] European Commission, Sweeps, available at: https://commission.europa.eu/topics/consumers/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en#ref-2020---sweeps-on-consumer-scams-related-to-the-covid-19-pandemic.

[1368] Hongliang Chen, Miao He, Xiaowen Xu and David Atkin, Examining Older Adults' Vulnerability to Online Health Scams: Insights from Routine Activity Theory (2025), available at: https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2025.1585851/full.

[1369] Adnan Kisa, Sezer Kisa., Health Conspiracy Theories: A Scoping Review of Drivers, Impacts, and Countermeasures (2025), available at: https://link.springer.com/article/10.1186/s12939-025-02451-0.

[1370] Rachel Moran et al., cited in The Political Economy of Wellness (2025), available at: https://onlinelibrary.wiley.com/doi/full/10.1111/1468-0009.70088?msockid=2d71bdae5bb16d580cd3aa205ab16c1c.

industry scandals, is systematically leveraged to encourage consumers to seek and purchase alternative products online.[1371]

Regulatory and policy sources similarly recognise the nexus between health conspiracies and fraud. The U.S. Food and Drug Administration identifies claims that cures are being suppressed by governments or 'Big Pharma' as a common indicator of health scams, noting that such narratives distract consumers from questioning the efficacy of purported miracle products.[1372] In the EU, the European Commission has acknowledged that manipulation, deceptive marketing, fraud and scams may converge with health conspiracies to exploit fears and market unnecessary, ineffective or potentially dangerous products under false health claims.[1373] A 2023 parliamentary question further highlighted the use of sponsored advertisements promoting dubious medicines and supplements with exaggerated claims, often relying on social media algorithms and misappropriated medical endorsements to redirect consumers – particularly older persons – to deceptive purchasing websites.[1374] The European Parliament Research Service has likewise documented the broader impact of health misinformation and disinformation, including anti-vaccine narratives, on public responses to vaccination campaigns, Ebola, cancer treatments and the COVID-19 pandemic.[1375] Another communication tactic for scammers is to market these products using unfair commercial practices such as scarcity claims ('lowest price', 'only available today', 'sells out fast').[1376]

Academic research finds that social media platforms, particularly Facebook, X, YouTube, WeChat, and TikTok, are major channels for the spread of health conspiracy theories, and their links to e-commerce marketplaces create an important pathway for consumer fraud.[1377] This strand of research claims that the recommendation systems of these platforms would prioritise emotionally engaging content, which may allow conspiracy

---

[1371] Bitdefender Labs, 'Deep Dive on Supplement Scams' (2024), available at: https://www.bitdefender.com/en-gb/blog/labs/deep-dive-on-supplement-scams-how-ai-drives-miracle-cures-and-sponsored-health-related-scams-on-social-media.

[1372] US Food and Drug Administration , 6 Tip-offs to Rip-offs: Don't Fall for Health Fraud Scams (2021), available at: https://www.fda.gov/consumers/consumer-updates/6-tip-offs-rip-offs-dont-fall-health-fraud-scams.

[1373] European Commission, Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions - Tackling Covid-19 Disinformation - Getting The Facts Right JOIN(2020) 8 final (2020), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0008.

[1374] European Parliament, Answer to Parliamentary Question E-000738/2023 (2023), available at: https://www.europarl.europa.eu/doceo/document/E-9-2023-000738-ASW_EN.html.

[1375] European Parliament Research Service, Countering the Health Infodemic (2020), available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/649369/EPRS_ATA(2020)649369_EN.pdf.

[1376] ACAMS, Fraud and Fear: COVID-19 Scams (2021), available at: https://www.acams.org/en/opinion/fraud-and-fear-covid-19-scams.

[1377] Yuwei Chuai, Jichang Zhao and Gabriele Lenzini, From News Source Sharers to Post Viewers: How Topic Diversity and Conspiracy Theories Shape Engagement With Misinformation During a Health Crisis (2024), available at: https://arxiv.org/pdf/2401.08832; Ruofei Chen, Guoyong Chen, Li Zhang, Ruiqian Xie and Ruopeng Chen, An Analysis of the Factors Influencing Engagement Metrics Within the Dissemination of Health Science Misinformation (2025), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12180413/.

narratives to spread faster than corrections – the report finds that conspiracy-related misinformation receives on average 40.8% more reposts, 45.2% more likes, and 44.1% more replies than comparable non-conspiracy content.[1378] During COVID-19, disinformation campaigns, bots, and wellness influencers exploited these dynamics to undermine trust in medical authorities and promote unproven alternatives.[1379] This misinformation often moves across multiple platforms. Conspiracy narratives can originate on social media, be amplified through recommendation systems and affiliate advertising networks, and ultimately drive sales on e-commerce marketplaces. For example, claims that governments suppress effective treatments can generate distrust on one platform, gain viral reach on another, and be monetised through fraudulent product listings elsewhere.[1380] This creates a self-reinforcing cycle in which health scams become both the commercial outcome and a perceived confirmation of the underlying conspiracy theory, with social media algorithms and misinformation networks directly contributing to consumer exploitation on e-commerce platforms.[1381]

On e-commerce platforms, health conspiracies, misinformation and scams can reinforce one another in a process that leads consumers from exposure to purchase: misinformation generates demand for alternative products, deceptive advertising and endorsements encourage purchases, and marketplace infrastructure facilitates transactions, while weak platform governance may allow similar products to persist across traders and listings.

Platform-level interventions

Across the VLOPs' reports assessed, mitigation measures addressing health and wellness scams are embedded within broader product safety and illegal content enforcement frameworks rather than constituting dedicated, health-specific intervention programs. All five e-commerce platforms taken into consideration for this specific scam (Amazon, Google Shopping, Temu, Shein, AliExpress) deploy multi-layered control architectures combining seller onboarding and verification, pre-listing automated screening (using keyword detection, image recognition, and machine-learning models), post-listing surveillance, and penalty-based enforcement systems.[1382] Common features include integration with the EU Safety Gate recall system, compliance documentation requirements for regulated product categories (including cosmetics and medicines), and escalating sanctions culminating in account termination for repeat offenders.[1383] Beyond

[1378] Yuwei Chuai, Jichang Zhao and Gabriele Lenzini, From News Source Sharers to Post Viewers: How Topic Diversity and Conspiracy Theories Shape Engagement With Misinformation During a Health Crisis (2024), available at: https://arxiv.org/pdf/2401.08832.

[1379] Sudip Bhattacharya and Alok Singh, Unravelling the Infodemic: A Systematic Review of Misinformation Dynamics During the COVID-19 Pandemic (2025), available at: https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2025.1560936/full; Emily Denniss and Rebecca Lindberg, Social Media and the Spread of Misinformation: Infectious and a Threat to Public Health (2025), available at: https://academic.oup.com/heapro/article/40/2/daaf023/8100645.

[1380] Adnan Kisa, Sezer Kisa, Health Conspiracy Theories: A Scoping Review of Drivers, Impacts, and Countermeasures' (2025), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC11969846/.

[1381] Sudip Bhattacharya and Alok Singh, Unravelling the Infodemic: A Systematic Review of Misinformation Dynamics During the COVID-19 Pandemic (2025), available at: https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2025.1560936/full.

[1382] Amazon, Shein, AliExpress, Google, Temu 2025 Risk Assessment Reports.

[1383] Temu, AliExpress, Amazon, Shein 2025 Risk Assessment Reports.

these commonalities, some unique approaches have also been identified on platforms like Google Shopping, AliExpress, or Temu.

For example, Google Shopping explicitly restricts the sale of pill presses and encapsulating machines (equipment directly associated with the manufacture of fraudulent health products) through its service.[1384] AliExpress reports imposing mandatory compliance certificate controls through which sellers are required to upload CE markings, declarations of conformity, and laboratory test reports for high-risk categories including cosmetics.[1385] Temu reports implementing a physical spot-check program involving accredited laboratory testing and in-person inspections.[1386]

None of the platforms describes a mitigation program specifically designed to detect and address the distinctive characteristics of health and wellness scams (such as misleading efficacy claims, unauthorised therapeutic indications, or deceptive before-and-after imagery) as distinct from general prohibited product enforcement.

Limitations of current measures and systemic challenges identified

None of the five e-commerce platforms in this case study treats health and wellness scams as an independent risk category warranting its own assessment framework, risk indicators, or dedicated enforcement metrics; instead, such risks are dispersed across Illegal Content, Prohibited and Controlled Products, Public Health, and Consumer Protection modules, creating fragmentation that may obscure the true scope of the problem. The absence of health-specific enforcement data is notable. While platforms report aggregate product removals and proactive interception rates, none discloses figures specifically attributable to health and wellness product violations (such as removals of misleading supplements, unauthorised cosmetics, or products bearing false therapeutic claims).

Risk classification varies across the platforms: Amazon and Shein characterise public health risk as essentially inapplicable to transactional marketplaces, asserting that such risks are more relevant to social media platforms, while AliExpress rates its Prohibited and Controlled Products inherent risk as High, and Temu assigns a Medium-High inherent risk to consumer protection encompassing economic harm from scams and fraud.[1387] The acknowledged capacity of recommender systems to amplify non-compliant products that evade initial screening, expressly recognised by AliExpress, Temu, and Google Shopping, represents an ongoing systemic vulnerability, particularly as algorithmic personalisation may direct health and wellness products toward users who have previously engaged with similar content.[1388]

Furthermore, it seems that a limitation of current countermeasures by e-commerce VLOPs is that they remain largely listing-, seller-, and notice-based, while the sale of

[1384] Google, 2025 Risk Assessment Report.

[1385] AliExpress, 2025 Risk Assessment Report.

[1386] Temu, 2025 Risk Assessment Report.

[1387] Amazon, Shein, AliExpress, Temu 2025 Risk Assessment Reports.

[1388] Google, Temu, AliExpress 2025 Risk Assessment Reports.

counterfeit and illegal medicines is organised across a wider online infrastructure.[1389] Seller verification, automated screening, brand-owner reporting tools, delisting, and repeat-offender policies can reduce the availability of obvious offers, but they do not consistently address shopping ads or the rapid re-entry of sellers under new identities.[1390] This creates an enforcement asymmetry: platforms can remove detected listings, but criminal sellers can shift channels, relist products, alter product descriptions, or route consumers to external sites faster than public authorities, rights holders, and medicine regulators can investigate and coordinate action.

This challenge is particularly acute for medicines because an effective compliance model requires more than generic counterfeit-goods detection: platforms must distinguish lawful online pharmacies and authorised retailers from unauthorised sellers, identify prescription-only or otherwise restricted products, recognise misleading health claims and disguised listings, and respond to public-health signals such as medicine shortages or sudden demand for products like GLP-1 medicines.[1391]

The convergence of health conspiracies and e-commerce also creates enforcement challenges, as existing regulatory frameworks were not designed for content that is simultaneously ideological and commercial. E-commerce moderation has traditionally focused on product safety, trademark infringement and prohibited listings rather than the accuracy of accompanying health claims. Research has shown that e-commerce platforms can facilitate the spread of health misinformation through both product listings and recommendation systems: an audit of Amazon found that over 10% of products returned for vaccine-related searches were misinformative and that recommendation systems could steer users towards increasingly conspiratorial content.[1392] Similarly, Brookings notes that the structure of online commerce makes it easy to market conspiracy-linked products while offering limited transparency into retailers' moderation practices.[1393]

Regulatory responses remain fragmented. Although the DSA recognises in Recital 83 that systemic risks may arise from public-health disinformation and algorithmic amplification, including information that is not itself illegal, it does not distinguish between ideological health misinformation and commercial scams exploiting such narratives. Enforcement therefore depends on whether content violates medicines, consumer-protection, product-safety or platform rules. This creates a gap: products promoted through implicit anti-pharmaceutical conspiracy narratives may contribute to consumer

[1389] Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/publications-events/publications/threat-of-pharmaceutical-crime-in-eu-and-beyond.

[1390] Eucrim, Europol Report: Pharmaceutical Crime in the EU (2025), available at: https://eucrim.eu/news/europol-report-pharmaceutical-crime-in-the-eu/; Eurojust, The threat of falsified medicines (2024), https://www.eurojust.europa.eu/publication/threat-falsified-medicines.

[1391] EMA, EU actions to tackle shortages of GLP-1 receptor agonists (2024), available at: https://www.ema.europa.eu/en/news/eu-actions-tackle-shortages-glp-1-receptor-agonists; EMA, Warning about sharp rise in illegal medicines sold in the EU (2025), available at: https://www.ema.europa.eu/en/news/warning-about-sharp-rise-illegal-medicines-sold-eu.

[1392] Prerna Juneja, Tanushree Mitra, Auditing E-Commerce Platforms for Algorithmically Curated Vaccine Misinformation (2021), available at: https://arxiv.org/abs/2101.08419.

[1393] Patrick Jones, The conspiracy and disinformation challenge on e-commerce platforms (2021), available at: https://www.brookings.edu/articles/the-conspiracy-and-disinformation-challenge-on-e-commerce-platforms/.

harm without clearly breaching existing legal thresholds. While the European Medicines Agency provides tools to address unauthorised or falsified medicines, including verified online-pharmacy schemes, these mechanisms do not extend to many supplements or wellness products that rely on conspiracy narratives without qualifying as medicinal products.[1394] Moreover, enhanced DSA systemic-risk obligations apply only to VLOPs and VLOSEs, leaving parts of the e-commerce ecosystem subject to more limited oversight.[1395] As a result, the intersection of health conspiracies and e-commerce scams remains an area where further guidance, platform transparency, and cooperation between medicines, consumer protection and digital services authorities may be warranted.

A major systemic challenge, therefore, is not simply insufficient takedown, but the absence of a consistently medicine-specific, cross-platform and cross-border risk model that links marketplace controls with pharmacy authorisation data, advertising oversight, customs intelligence, payment and logistics signals, and rapid law-enforcement escalation.[1396]

Conclusions and recommendations

The case study shows that health and wellness scams on e-commerce platforms are a systemic marketplace risk at the intersection of consumer fraud, product safety, public health, and organised crime.

Counterfeit and illegal medicines, fraudulent supplements, unsafe cosmetics, and deceptive wellness products exploit the same structural features that make e-commerce platforms efficient: rapid seller onboarding, scalable listing creation, sponsored placement, algorithmic ranking, review-based trust signals, integrated payment and fulfilment systems, and cross-border parcel logistics. The evidence also shows that scammers adapt quickly, using official-looking logos, false endorsements, misleading health claims, manipulated reviews, scarcity cues, AI-generated advertising content, and third-country fulfilment structures to create consumer trust and evade enforcement.

While VLOPs have introduced some countermeasures (including seller verification, automated screening, notice-and-action systems, Safety Gate integration, product testing, documentation requirements, and account sanctions), these measures remain largely embedded in general illegal-product or product-safety frameworks. They do not yet amount to a consistently health-specific risk model capable of detecting misleading therapeutic claims, unauthorised medicines, disguised prescription-only products, or fast-moving scam campaigns linked to public-health demand shocks such as COVID-19 or GLP-1 shortages. The key insight is therefore that the regulatory challenge is not only one of removing unlawful listings faster, but of requiring platforms to assess and mitigate the full e-commerce pathway through which these scams operate: discovery, ranking, advertising, seller identity, product claims, reviews, payment, fulfilment, recall, and repeat seller re-entry.

[1394] European Medicine Agency, Buying medicines online, available at: https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview/buying-medicines-online.

[1395] European Parliament, Problems presented by third-country e-commerce (2025), available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/767224/EPRS_BRI(2025)767224_EN.pdf.

[1396] Eurojust, The threat of falsified medicines (2024), https://www.eurojust.europa.eu/publication/threat-falsified-medicines.

Because no standard best practices or actionable recommendations could be identified at this stage, this topic warrants further targeted investigation by relevant stakeholders to develop effective interventions.

7. Conclusions

The findings of this study paint a picture of an online financial scam landscape that is growing in scale and in its structural complexity. Across the six categories of scams examined, a set of recurring dynamics emerges that transcends individual scam typologies and points to deeper, systemic features of the digital environment that enable and sustain fraudulent activity. This concluding section draws out those overarching themes, reflects on their broader implications, identifies the research gaps that remain, and considers the directions in which future inquiry might most productively develop.

Overarching themes and key insights

Perhaps the most significant finding of this study is the extent to which online financial scams are structurally embedded within the ordinary functioning of designated services. Scammers are not merely exploiting isolated vulnerabilities. They operate through the same advertising systems, recommendation algorithms, account creation processes, monetisation models, and private messaging functionalities that legitimate users rely upon. It becomes apparent that the infrastructure of digital platforms, designed to facilitate reach, engagement, and commercial activity, serves fraudulent purposes with comparable efficiency. The evidence cited throughout this report suggests that the design logic of platforms, particularly the prioritisation of engagement, low-friction onboarding, and scalable content distribution, may create conditions that are structurally conducive to scam operationalisation.

A second overarching theme is the increasing hybridisation and adaptability of scam models. For example, the emergence of romance baiting, which fuses the trust-building techniques of romance scams with the financial extraction mechanisms of investment fraud, illustrates how scammers combine elements from different typological categories to construct schemes that evade both victim recognition and platform detection. This adaptive behaviour extends to the strategic selection of platforms, the exploitation of trending content, and the rapid adjustment of techniques in response to enforcement actions. The study's findings suggest that static, category-based approaches to scam classification and detection are increasingly insufficient. Scam models are converging, and detection systems that treat each typology in isolation risk missing the hybrid configurations that now characterise the most sophisticated operations.

Third, the study reveals a pronounced asymmetry between the sophistication of scam operations and the capacity of existing countermeasures to respond. Fraudsters benefit from industrialised criminal infrastructure, including fraud-as-a-service markets, commercially available deepfake tools, phishing kits, and bot networks, that dramatically lowers the barrier to entry and enables operations at scale. Meanwhile, platform countermeasures, though widespread, remain primarily reactive and content-focused. The evidence points to a potential gap: platforms tend to address scam content at the level of individual advertisements, posts, or accounts, while the underlying networks, infrastructure, and repeat offenders that sustain scam campaigns often remain intact.

It is posited that the cross-platform nature of online financial scams fundamentally complicates prevention and enforcement. The study identifies recurrent migration pathways through which scams move from paid advertisements or organic social media content to private messaging applications, and ultimately to fraudulent external websites. No single platform controls the entire scam chain, and enforcement actions on one service may result in displacement rather than cessation. This fragmentation means that effective countermeasures must account for the interconnected ecosystem through which scams are operationalised.

Finally, the study's findings on the social and economic impact of online financial scams underscore that the harm extends far beyond immediate financial loss. The psychological consequences, including shame, anxiety, depression, post-traumatic stress, and, in the most severe cases, suicidal ideation, are compounded by a culture of victim-blaming and a lack of adequate support structures. The erosion of consumer trust in online platforms and digital commerce represents a systemic harm that affects not only individual victims but the functioning of the internal market itself. These impacts are unevenly distributed, with financially vulnerable individuals, those experiencing loneliness or emotional distress, younger people drawn to speculative digital environments, and older adults with limited digital literacy bearing disproportionate burdens.

Critical reflections

The findings of this study invite critical reflection on several dimensions of the current regulatory and enforcement landscape. The Digital Services Act establishes a framework in which designated services are required to assess and mitigate systemic risks, including the dissemination of illegal content and negative effects on fundamental rights. The evidence gathered in this study preliminarily suggests that while platforms have developed countermeasure strategies, the translation of those measures into effective, measurable reductions in scam prevalence and impact remains difficult to establish. This raises important questions about whether current enforcement models are calibrated to the scale and speed at which scam operations function.

A further point of reflection concerns the structural incentives that shape platform behaviour. The research efforts collected claims from stakeholders that advertising revenue derived from fraudulent content may create a tension between commercial interests and user protection. While these claims require careful interpretation, they raise important points for consideration in evaluating the trade-offs platforms accept.

The role of AI in the scam landscape also warrants critical consideration. The study concludes that AI operates primarily as a transformative amplifier of existing scam models. AI-generated deepfakes, automated social engineering, multilingual content production, and real-time adaptation to detection systems collectively shift the balance between scam operators and the enforcement mechanisms designed to counter them. The steps towards the development of interoperable AI-content labelling and detection standards across platforms highlight a mutual understanding of the need for coordinated efforts.

Future research directions

Despite the breadth of this study, a number of significant evidence gaps remain. First, the true scale and prevalence of online financial scams across the European Union are not known with any precision. Under-reporting is endemic, with estimates suggesting that only around 15% of victims report scams. The absence of harmonised, EU-wide data collection on scam incidence, typology, and financial loss makes it impossible to establish reliable baselines. Without such baselines, the question of whether platform interventions are reducing scam prevalence remains difficult to answer.

The relationship between platform design features, particularly recommender systems, and the amplification of scam content is still not fully understood. While theoretical models and indirect evidence suggest that engagement-maximising algorithms can surface fraudulent material, no large-scale empirical study has established causal links between specific algorithmic configurations and measurable increases in user exposure to scams. The limited transparency of proprietary recommendation systems represents a fundamental obstacle to research in this area.

Moreover, data on the economic impact of specific scam types at EU level is fragmentary and inconsistent. For several categories, including insurance scams, fake job scams, charity scams, and crowdfunding fraud, no reliable European-level loss estimates exist. Where national data is available, methodological differences in measurement and reporting make cross-country comparison difficult. The study's reliance on self-reported survey data, official crime statistics, and investigative case studies produces an evidence base that is indicative rather than comprehensive.

The effectiveness of individual countermeasures remains largely unquantified. Platforms do not generally publish metrics such as false-negative rates, precision, or recall for their automated detection systems, nor do they disclose the proportion of user reports that receive human review or the outcomes of that review. This absence of performance data makes it difficult to identify which measures are most effective and where investment should be directed.

Lastly, the victimology of online financial scams requires further development. While the study identifies broad demographic and behavioural patterns of vulnerability, the mechanisms through which platform design interacts with individual psychological characteristics to produce victimisation are not well understood. In particular, the role of repeated algorithmic exposure in normalising implausible claims and gradually lowering user vigilance is a hypothesis that has not been empirically tested at scale.

In sum, this study provides a comprehensive mapping of the online financial scam landscape as it stands in 2026. The picture that emerges is one of a phenomenon that is deeply embedded in the architecture of digital platforms, increasingly industrialised in its operational infrastructure, and growing in both its economic and human toll. The findings underline the need for sustained, evidence-based, and coordinated action that addresses not only the symptoms of online financial scams but also the structural conditions that enable them to persist and proliferate.

8. Annexes

- Annex I – List of sources
- Annex II – Interview guide for Task 1
- Annex III – Interview guide for Task 2
- Annex IV – Workshop Report
- Annex V – Overview of measures implemented by designated service providers

Annex I – List of sources

EU Publications

- ECB, Joint EBA-ECB report on payment fraud: strong authentication remains effective, but fraudsters are adapting (2025), available at: https://www.ecb.europa.eu/press/pr/date/2025/html/ecb.pr251215~e133d9d683.en.html
- EDMO, Meta's Failure to Curb Digital Scams: The Alarming Spread of Fraud on Facebook and Instagram in the EU (2025), available at: https://edmo.eu/publications/metas-failure-to-curb-digital-scams-the-alarming-spread-of-fraud-on-facebook-and-instagram-in-the-eu/
- ENISA, ENISA Threat Landscape 2025 (2026), available at: https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
- ENISA, ENISA Threat Landscape 2024 (2024), available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
- ESMA, ESMA highlights risks to retail investors of social media driven share trading (2021), available at: https://www.esma.europa.eu/press-news/esma-news/esma-highlights-risks-retail-investors-social-media-driven-share-trading.
- ESMA, ESMA urges social media companies to tackle unauthorised financial ads (2025), available at: https://www.esma.europa.eu/press-news/esma-news/esma-urges-social-media-companies-tackle-unauthorised-financial-ads
- ESMA, Warning on Social Media and Investment Recommendations (2024), available at: https://www.esma.europa.eu/sites/default/files/2024-02/ESMA74-1103241886-912_Warnings_on_Social_Media_and_Investment_Recommendations.pdf.
- Eurojust, Decisive actions against cryptocurrency scammers earning over EUR 600 million (2025), available at: https://www.eurojust.europa.eu/news/decisive-actions-against-cryptocurrency-scammers-earning-over-eur-600-million
- Eurojust, The threat of falsified medicines (2024), available at: https://www.eurojust.europa.eu/publication/threat-falsified-medicines
- European Banking Authority, EBA Opinion on new types of payment fraud and possible mitigants (2024), available at: https://eba.europa.eu/sites/default/files/2024-04/363649ff-27b4-4210-95a6-0a87c9e21272/Opinion%20on%20new%20types%20of%20payment%20fraud%20and%20possible%20mitigations.pdf
- European Banking Authority, Fraudes et Escroqueries Liées aux Crypto-Actifs : Restez Vigilant(E) et Protégez-Vous, available at: https://www.cssf.lu/wp-content/uploads/Fraudes-et-escroqueries-liees-aux-crypto-actifs.pdf
- European Board for Digital Services, Second Report of the European Board for Digital Services in cooperation with the Commission pursuant to Article 35(2) DSA on the most prominent and recurrent systemic risk as well as mitigation measures (2026), available at: https://digital-strategy.ec.europa.eu/en/library/second-report-systemic-risks-very-large-online-platforms-and-search-engines-under-digital-services

- European Central Bank, Instant Payments Regulation, available at: https://www.ecb.europa.eu/paym/retail/instant_payments/html/instant_payments_regulation.en.html
- European Commission, 2024 Consumer conditions survey – Full data set (2025), available at: https://commission.europa.eu/publications/2024-consumer-conditions-survey-full-data-set_en
- European Commission, 2030 Consumer Agenda and Action Plan for Consumers in the Single Market – A New Impulse for Consumer Protection, Competitiveness and Sustainable Growth (2025), available at: https://commission.europa.eu/document/download/84cfc60e-f264-4f31-9f79-9ec83dce064d_en?filename=JUST_template_comingsoon_standard_14.pdf.
- European Commission, Code of Practice on Transparency of AI-Generated Content (2026), available at: https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content
- European Commission, Commission Decision of 5.12.2025 pursuant to Articles 73(1), 73(3) and 74(1) of Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act) Cases DSA.100101, DSA.100102 and DSA.100103 – X (formerly Twitter) (2025), available at: https://ec.europa.eu/newsroom/dae/redirection/document/128762
- European Commission, Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act (2024), available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373
- European Commission, Commission Preliminarily Finds TikTok and Meta in Breach of Their Transparency Obligations Under the Digital Services Act (2025), available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2503
- European Commission, Commission Staff Working Document on EU Consumer Law on Digital Fairness (2024), available at: https://commission.europa.eu/document/707d7404-78e5-4aef-acfa-82b4cf639f55_en
- European Commission, Consumer Conditions Scoreboard (2025), available at: https://commission.europa.eu/document/download/2816337b-4fd1-4db2-a71c-d14a206a5a93_en?filename=consumer_conditions_scoreboard_2025_final.pdf
- European Commission, Consumer Protection Cooperation Network, available at: https://commission.europa.eu/topics/consumers/consumer-rights-and-complaints/enforcement-consumer-protection/consumer-protection-cooperation-network_en
- European Commission, E-commerce communication: a comprehensive EU toolbox for safe and sustainable e-commerce (2025), available at: https://digital-strategy.ec.europa.eu/en/library/e-commerce-communication-comprehensive-eu-toolbox-safe-and-sustainable-e-commerce
- European Commission, European Digital Identity (EUDI) Regulation (2026), available at: https://digital-strategy.ec.europa.eu/en/policies/eudi-regulation.
- European Commission, Fighting Online Scams with DSA (2025), available at https://digital-strategy.ec.europa.eu/en/policies/dsa-notice-and-action-mechanism.

- European Commission, How the Digital Services Act Enhances Transparency Online (2026), available at: https://digital-strategy.ec.europa.eu/en/policies/dsa-brings-transparency
- European Commission, Joint Communication To The European Parliament, The European Council, The Council, The European Economic And Social Committee And The Committee Of The Regions - Tackling Covid-19 Disinformation - Getting The Facts Right JOIN(2020) 8 final (2020), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020JC0008
- European Commission, Study on online identity theft and identity-related crime – Final report (2022), available at: https://op.europa.eu/en/publication-detail/-/publication/f85399b3-abed-11ec-83e1-01aa75ed71a1/language-en
- European Commission, Supervision of the designated very large online platforms and search engines under DSA, available at: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses#ecl-inpage-google
- European Commission, Survey on “Scams and Fraud Experienced by Consumers", Final Report (2020), available at: https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf
- European Commission, Trusted Flaggers under the Digital Services Act (DSA) (2026), available at: https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa
- European Commission, Sweeps, available at: https://commission.europa.eu/topics/consumers/consumer-rights-and-complaints/enforcement-consumer-protection/sweeps_en#ref-2020---sweeps-on-consumer-scams-related-to-the-covid-19-pandemic
- European Medicines Agency, Buying medicines online, available at: https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview/buying-medicines-online
- European Medicines Agency, EU actions to tackle shortages of GLP-1 receptor agonists (2024), available at: https://www.ema.europa.eu/en/news/eu-actions-tackle-shortages-glp-1-receptor-agonists
- European Medicines Agency, Warning about sharp rise in illegal medicines sold in the EU (2025), available at: https://www.ema.europa.eu/en/news/warning-about-sharp-rise-illegal-medicines-sold-eu
- European Parliament, Answer to Parliamentary Question E-000738/2023 (2023), available at: https://www.europarl.europa.eu/doceo/document/E-9-2023-000738-ASW_EN.html
- European Parliament, Finfluencers: Setting Standards in a High-Risk Environment (2026), available at: https://www.europarl.europa.eu/news/en/agenda/plenary-news/2026-04-27/18/finfluencers-setting-standards-in-a-high-risk-environment
- European Parliament, Problems presented by third-country e-commerce (2025), available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/767224/EPRS_BRI(2025)767224_EN.pdf

- European Parliament, Report on product safety and regulatory compliance in e-commerce and non-EU imports (2025), available at: https://www.europarl.europa.eu/doceo/document/A-10-2025-0133_EN.html
- European Parliament Research Service, Countering the Health Infodemic (2020), available at: https://www.europarl.europa.eu/RegData/etudes/ATAG/2020/649369/EPRS_ATA(2020)649369_EN.pdf
- European Union, Better Internet for Kids – Sextortion (n.d.), available at: https://better-internet-for-kids.europa.eu/en/learning-corner/teachers-and-educators/sextortion
- European Union, Charter of Fundamental Rights of the European Union (2012), available at: https://eur-lex.europa.eu/eli/treaty/char_2012/oj/eng
- European Union, Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (2022), available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj/eng
- European Union, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act) (2024), available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
- European Union, Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive') (2005), available at: https://eur-lex.europa.eu/eli/dir/2005/29/oj/eng
- European Union, Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU (2014), available at: https://eur-lex.europa.eu/eli/dir/2014/65/oj/eng
- European Union, Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC (2008), available at: https://eur-lex.europa.eu/eli/dir/2008/48/oj/eng
- European Union, Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (consolidated text), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02010L0013-20250208
- European Union, Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (2024), available at: https://eur-lex.europa.eu/eli/reg/2024/900/oj/eng
- European Union Agency for Fundamental Rights, Crime, safety and victims' rights (2021), available at:

https://fra.europa.eu/sites/default/files/fra_uploads/fra-2021-crime-safety-victims-rights_en.pdf

- European Union Agency for Fundamental Rights, Online fraud – people's experiences across the EU (2026), available at: https://fra.europa.eu/en/publication/2026/victims-online-fraud
- European Union Intellectual Property Office, Apps and App Stores – Challenges and Good Practices to Prevent the Use of Apps and App Stores for IP Infringement Activities (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Apps_and_App_stores/2024_Apps_and_App_stores_FullR_en.pdf
- European Union Intellectual Property Office, EU Enforcement of Intellectual Property Rights – Results at the EU Border and in the EU Internal Market 2024 (2025), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2025_EU_Enforcement_report/EU_enforcement_of_IPRs:_results_at_EU_border_&_EU_internal_market_2024_en.pdf
- European Union Intellectual Property Office, Monitoring and analysing social media in relation to IP infringement (2021), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2021_Monitoring_and_analysing_social_media_in_relation_to_IPR_Infringement_Report/2021_Monitoring_and_analysing_social_media_in_relation_to_IPR_Infringement_Report_FullR_en.pdf
- European Union Intellectual Property Office, Search Engines – Challenges and Good Practices to Limit Search Traffic Towards Intellectual Property Infringing Content and Services (2024), available at: https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/2024_Search_Engines/2024_Search_Engines_FullR_en.pdf
- Europol, Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests (2022), available at: https://www.europol.europa.eu/media-press/newsroom/news/action-against-criminal-website-offered-%E2%80%98spoofing%E2%80%99-services-to-fraudsters-142-arrests
- Europol, Busted: 9 arrested in hit against holiday-rental fraudsters (2024), available at: https://www.europol.europa.eu/media-press/newsroom/news/busted-9-arrested-in-hit-against-holiday-rental-fraudsters
- Europol, Criminal Phishing Network Resulting in Over 480,000 Victims Worldwide Busted in Spain and Latin America (2024), available at: https://www.europol.europa.eu/media-press/newsroom/news/criminal-phishing-network-resulting-in-over-480-000-victims-worldwide-busted-in-spain-and-latin-america
- Europol, EMPACT (2026), available at: https://www.europol.europa.eu/how-we-work/empact
- Europol, Europol Spotlight – Cryptocurrencies: tracing the evolution of criminal finances (2022), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

- Europol, Europol Spotlight – Online fraud schemes: a web of deceit (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/e914d7fe-b429-11ee-b164-01aa75ed71a1/language-en
- Europol, Europol warns consumers to be mindful about fake medicines offered online (2025), available at: https://www.europol.europa.eu/media-press/newsroom/news/europol-warns-consumers-to-be-mindful-about-fake-medicines-offered-online
- Europol, Franco-Israeli gang behind EUR 38 million CEO fraud busted (2023), available at: https://www.europol.europa.eu/media-press/newsroom/news/franco-israeli-gang-behind-eur-38-million-ceo-fraud-busted
- Europol, Further action against fraudulent online investment platform: five arrests of high-value targets (2023), available at: https://www.europol.europa.eu/media-press/newsroom/news/further-action-against-fraudulent-online-investment-platform-five-arrests-of-high-value-targets
- Europol, International investigation disrupts phishing-as-a-service platform LabHost (2024), available at: https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost
- Europol, Internet Organised Crime Threat Assessment (IOCTA) 2023 (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/238c0013-26a9-11ee-a2d3-01aa75ed71a1/language-en
- Europol, Internet Organised Crime Threat Assessment 2025 (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf
- Europol, IOCTA 2024 – Internet Organised Crime Threat Assessment (2024), available at: https://op.europa.eu/en/publication-detail/-/publication/f7e2258d-4b04-11ef-acbc-01aa75ed71a1/language-en
- Europol, Money Muling (2025), available at: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling
- Europol, Operation Shield (2025), available at: https://www.europol.europa.eu/how-we-work/operations/operation-shield
- Europol, Protect yourself from holiday and ticket fraud (2021), available at: https://www.europol.europa.eu/2good2btrue
- Europol, Romance scams: recognising manipulation before it escalates (2026), available at: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/romance-scams-recognising-manipulation-it-escalates
- Europol, Serious and organised crime threat assessment – The changing DNA of serious and organised crime (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf
- Europol, The other side of the coin – An analysis of financial and economic crime (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/83f3cef9-5769-11ee-9220-01aa75ed71a1/language-en

- Europol, The threat of pharmaceutical crime in the EU and beyond (2025), available at: https://www.europol.europa.eu/cms/sites/default/files/documents/The_threat_of_pharmaceutical_crime_in_the_EU_and_beyond.pdf
- Europol-EUIPO, Uncovering the ecosystem of intellectual property crime: A focus on enablers and impact (2024), available at: https://www.europol.europa.eu/publications-events/publications/uncovering-ecosystem-of-intellectual-property-crime
- OECD and European Union Intellectual Property Office, Misuse of E-Commerce for Trade in Counterfeits (2021), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2021/10/misuse-of-e-commerce-for-trade-in-counterfeits_dfd7df43/1c04a64e-en.pdf

International Organisation Publications

- Council of Europe, Regulating content moderation on social media to safeguard freedom of expression (2025), available at: https://pace.coe.int/pdf/b11c97ecb434dedaec11f776b5c93c3dc5031b006e0be15e71c1e47227a78873/doc.%2016089.pdf
- FATF, Cyber-enabled fraud (2026), available at: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/cyber-enabled-fraud-digitalisation-ml-tf-pf-risks.html
- FATF, Egmont Group and INTERPOL, Illicit Financial Flows from Cyber-Enabled Fraud (2023), available at: https://www.fatf-gafi.org/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html.
- International Chamber of Commerce and GASA, Best practices for combating scams in advertising (2026), available at: https://iccwbo.org/wp-content/uploads/sites/3/2026/06/2026_ICC_GASA_Best_Practices_for_Combating_Scams_in_Advertising_EN.pdf
- International Organization of Securities Commissions (IOSCO), Finfluencers (2025), available at: https://www.iosco.org/library/pubdocs/pdf/IOSCOPD795.pdf
- International Organization of Securities Commissions (IOSCO), IOSCO's Statement on Combating Online Harm and the Role of Platform Providers (2025), available at: https://www.iosco.org/news/pdf/IOSCONEWS770.pdf
- Interpol, Global Financial Fraud Assessment (2024), available at: https://www.interpol.int/en/News-and-Events/News/2024/INTERPOL-Financial-Fraud-assessment-A-global-threat-boosted-by-technology
- Interpol, INTERPOL Releases New Information on Globalization of Scam Centres (2025), available at: https://www.interpol.int/en/News-and-Events/News/2025/INTERPOL-releases-new-information-on-globalization-of-scam-centres
- Interpol, Operation Pangea – shining a light on pharmaceutical crime (2019), available at: https://www.interpol.int/News-and-Events/News/2019/Operation-Pangea-shining-a-light-on-pharmaceutical-crime
- Interpol, Record 769 arrests and USD 65 million in illicit pharmaceuticals seized in global bust (2025), available at: https://www.interpol.int/en/News-and-

Events/News/2025/Record-769-arrests-and-USD-65-million-in-illicit-pharmaceuticals-seized-in-global-bust

- OECD, Illicit Trade: Converging Criminal Networks (2022), available at: https://books.google.be/books/about/Illicit_Trade.html?id=g8MFkAEACAAJ&redir_esc=y
- OECD, Mapping Global Trade in Fakes 2025 (2025), available at: https://www.oecd.org/en/publications/mapping-global-trade-in-fakes-2025_94d3b29f-en.html
- OECD, Protecting Consumers from Financial Scams and Frauds (2026), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2026/06/protecting-consumers-from-financial-scams-and-frauds_3887b249/d41817bb-en.pdf
- OECD, The Role of Online Marketplaces in Protecting and Empowering Consumers (2022), available at: https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/07/the-role-of-online-marketplaces-in-protecting-and-empowering-consumers_07af735e/9d8cc586-en.pdf
- Office of the United Nations High Commissioner for Human Rights (OHCHR), Hundreds of Thousands Trafficked into Online Criminality in Southeast Asia (2023), available at: https://www.ohchr.org/en/press-releases/2023/08/hundreds-thousands-trafficked-work-online-scammers-se-asia-says-un-report
- UN Office on Drugs and Crime, Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia (2025), available at: https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf
- UN Office on Drugs and Crime, Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape (2024), available at: https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf
- United Nations News, Global Scam Centres Expand Rapidly, Threatening Millions Worldwide (2026), available at: https://news.un.org/en/story/2026/02/1167012

National Authority Publications

- AFM, Investment fraud: losses likely in the hundreds of millions of euros per year (2025), available at: https://www.afm.nl/en/sector/actueel/2025/dec/pb-beleggingsfraude
- Australian National Anti-Scam Centre, Targeting Scams – Report of the National Anti-Scam Centre on scams data and activity 2025 (2026), available at: https://www.nasc.gov.au/system/files/targeting-scams-report-2025.pdf
- Autorité de contrôle prudentiel et de résolution (ACPR), L'ACPR met en garde le public contre la multiplication de fausses offres de prêt immobilier (2024), available at: https://acpr.banque-france.fr/fr/communiques-de-presse/lacpr-met-

en-garde-le-public-contre-la-multiplication-de-fausses-offres-de-pret-immobilier-ou-de

- Autorité des Marchés Financiers (AMF), Social Media Intelligence: Arnaques à l'investissement sur le web (2024), available at: https://www.amf-france.org/sites/institutionnel/files/private/2024-12/opinionway-pour-amf-les-arnaques-sur-le-web_octobre-2024_0.pdf
- Autoriteit Consument en Markt (ACM), Consumer organizations warn against untrustworthy online stores (2023), available at: https://www.acm.nl/en/publications/consumer-organizations-warn-against-untrustworthy-online-stores
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Investitionen in Kryptowerte und der Einfluss sozialer Medien auf das Anlageverhalten (2026), available at: https://www.bafin.de/DE/Aufsicht/Fokusrisiken/Fokusrisiken_2026/RIF_verbraucher_sozialemedien/RIF_verbraucher_sozialemedien_node.html
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Anlagebetrug über WhatsApp und Telegram, available at: https://www.bafin.de/DE/verbraucherinnen-verbraucher/themen-finanzprodukte/finanzbetrug-erkennen/anlagebetrug/whatsapp-telegram/whatsapp-telegram.html
- Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin), Memecoins: Glücksspiel statt Geldanlage, available at: https://www.bafin.de/DE/verbraucherinnen-verbraucher/themen-finanzprodukte/finanzbetrug-erkennen/anlagebetrug/memecoins/memecoins_node.html
- Bundesnetzagentur, Bundesnetzagentur helps make online shopping safer (2025), available at: https://www.bundesnetzagentur.de/SharedDocs/Pressemitteilungen/EN/2025/20251128_DSC.html
- Competition and Consumer Protection Commission (CCPC), Scams – Real cases, real consequences: A collection of case studies and lessons for consumers (2025), available at: https://www.ccpc.ie/consumers/wp-content/uploads/sites/2/2025/11/Scams-Real-cases-real-consequences-CCPC.pdf
- DC Department of Insurance, Securities and Banking, Warning Signs of a Penny Stock Scam, available at: https://disb.dc.gov/page/warning-signs-penny-stock-scam
- Direction générale de la Concurrence, de la Consommation et de la Répression des fraudes (DGCCRF), Arnaques financières : les autorités mobilisées dans la lutte contre ce phénomène massif (2024), available at: https://www.economie.gouv.fr/files/files/directions_services/dgccrf/media-document/cp-dgccrf-conference-afm.pdf
- eSafety Commissioner Australia, Position statement – Recommender systems and algorithms (2023), available at: https://www.esafety.gov.au/industry/tech-trends-and-challenges/recommender-systems-and-algorithms/full-position-statement

- FBI, International Law Enforcement Agencies Issue Joint Warning about Global Financial Sextortion Crisis (2023), available at: https://www.fbi.gov/news/press-releases/international-law-enforcement-agencies-issue-joint-warning-about-global-financial-sextortion-crisis
- Financial Arbiter of Malta, Technical Note – Follow Up (January 2026), available at: https://financialarbiter.org.mt/sites/default/files/Technical%20Note%20-%20Follow%20Up%20-%20Jan%202026%20%5BFinal%5D_0.pdf
- Financial Services and Market Authority (FSMA), Investment fraud and unlawful offers – Dashboard 2nd half of 2025 (2026), available at: https://www.fsma.be/sites/default/files/media/files/2026-01/20260122_dashboard_investment_fraud_2025_s2.pdf
- Financial Services and Market Authority (FSMA), Opgelet voor beleggingstips via WhatsApp (2026), available at: https://www.fsma.be/nl/warnings/opgelet-voor-beleggingstips-whatsapp
- Financial Services and Market Authority (FSMA), Received an interesting credit offer? Be careful! (2025), available at: https://www.fsma.be/en/warnings/received-interesting-credit-offer-be-careful
- Financial Services and Market Authority (FSMA), Cloned firms: theft of the identity of authorized companies, available at: https://www.fsma.be/en/cloned-firms-theft-identity-authorized-companies
- Finans Danmark, Styrket bekæmpelse af digital svindel - Svindel Task Forcens 18 anbefalinger (2024), available at: https://www.ft.dk/samling/20241/almdel/ERU/bilag/81/2948819/index.htm
- Fraudehelpdesk, In 2023 bedroeg schade datingfraude méér dan 7 miljoen euro (2024), available at: https://www.fraudehelpdesk.nl/wp-content/uploads/2024/02/Persbericht-campagne-datingfraude-5-2-24.pdf
- Health Products Regulatory Authority (HPRA), Urgent warning of fraudulent websites and adverts promoting illegal medicines (2025), available at: https://www.hpra.ie/news-events/news/article/urgent-warning-of-fraudulent-websites-and-adverts-promoting-illegal-medicines
- Internet Crime Complaint Center (IC3), Deepfakes and Stolen PII Utilized to Apply for Remote Work Positions (2022), available at: https://www.ic3.gov/PSA/2022/psa220628
- IRS, IRS assesses $162 million in penalties over false tax credit claims tied to social media (2025), available at: https://www.irs.gov/newsroom/irs-assesses-162-million-in-penalties-over-false-tax-credit-claims-tied-to-social-media
- Nederlandse Politie, Politie waarschuwt met nepwebsite voor ticketfraude (2026), available at: https://www.politie.nl/nieuws/2026/januari/15/politie-waarschuwt-met-nepwebsite-voor-ticketfraude.html
- OCC (Spain), Informe sobre la cibercriminalidad en España (2024), available at: https://occ.ses.mir.es/publico/occ/dam/jcr:b9a4f43b-88c7-48f9-ab12-9b6891288b4c/Informe-sobre-la-cibercriminalidad-en-Espa%C3%B1a-2024.pdf
- Ofcom, Scale and impact of online fraud revealed (2023), available at: https://www.ofcom.org.uk/online-safety/online-fraud/scale-and-impact-of-online-fraud-revealed
- OSMP, Rapport de l'Observatoire de la sécurité des moyens de paiement 2024 (2024), available at: https://www.banque-france.fr/fr/publications-et-

statistiques/publications/rapport-de-lobservatoire-de-la-securite-des-moyens-de-paiement-2024

- Poliisi (Finland), Information and open discussion are key factors in combatting online scams (2026), available at: https://poliisi.fi/en/-/information-and-open-discussion-are-key-factors-in-combatting-online-scams
- Polisen (Sweden), Bedrägeribrottslighetens vinster sjunker för andra året i rad (2026), available at: https://polisen.se/aktuellt/nyheter/nationell/2026/april/bedrageribrottslighetens-vinster-sjunker-for-andra-aret-i-rad/
- Polisen (Sweden), Brottsvinsterna för bedrägeribrottsligheten 2025 (2026), available at: https://polisen.se/e138feea53c6c74289ea158bf6059519/siteassets/dokument/ovriga_rapporter/brottsvinsterna-for-bedrageribrottsligheten-2025.pdf
- Safeonweb, Beware of inheritance fraud: reports of unexpected inheritances are doing the rounds again (2025), available at: https://safeonweb.be/en/news/beware-inheritance-fraud-reports-unexpected-inheritances-are-doing-rounds-again
- Scamwatch, Beware of fake lottery and competition 'wins' on social networking platforms (2015), available at: https://www.scamwatch.gov.au/about-us/news-and-alerts/alerts-bulletins/investor-alerts/social-media-and-investment-fraud-investor-alert
- Scamwatch, Unexpected money scams, available at: https://www.scamwatch.gov.au/types-of-scams/unexpected-money-scams
- Singapore Government, ScamShield, available at: https://www.scamshield.gov.sg/
- UK CMA, Undertaking relating to Amazon (2025), available at: https://assets.publishing.service.gov.uk/media/6841a7ca578282a4b102c0ab/Amazon_s_undertaking_to_the_CMA_.pdf
- UK CMA, Undertaking relating to Google (2025), available at: https://assets.publishing.service.gov.uk/media/67924902e982ca138427fc1e/Google_s_undertaking_to_the_CMA.pdf
- UK Financial Conduct Authority, Protect yourself from scams (2026), available at: https://www.fca.org.uk/consumers/protect-yourself-scams
- UK Government, £1.6m lost to gig ticket scams as public urged to take caution (2025), available at: https://www.gov.uk/government/news/16m-lost-to-gig-ticket-scams-as-public-urged-to-take-caution
- UK Home Office, Economic Crime Survey (2025), available at: https://www.gov.uk/government/publications/economic-crime-survey-2024/economic-crime-survey-2024
- UK National Fraud Authority, Fraud typologies and victims of fraud – Literature review (2009), available at: https://assets.publishing.service.gov.uk/media/5a7ad8c2ed915d670dd7efad/fraud-typologies.pdf
- UK Parliament – Science, Innovation and Technology Committee, Social media, misinformation and harmful algorithms (2025), available at: https://committees.parliament.uk/publications/48745/documents/258221/default/

- UK Payment Systems Regulator, APP Fraud Reimbursement Protections (2024), available at: https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/
- UK Report Fraud, available at: https://www.reportfraud.police.uk/.
- US Federal Bureau of Investigation, Internet Crime Report 2024, available at: https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf.
- US Federal Trade Commission, Reported losses to scams on social media eight times higher than in 2020 (2026), available at: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2026/04/reported-losses-scams-social-media-eight-times-higher-2020#ft5
- US Federal Trade Commission, ICPEN and GPEN, Results of Review of Use of Dark Patterns Affecting Subscription Services (2024), available at: https://www.ftc.gov/news-events/news/press-releases/2024/07/ftc-icpen-gpen-announce-results-review-use-dark-patterns-affecting-subscription-services-privacy.
- US Federal Trade Commission, Trade Regulation Rule on the Use of Consumer Reviews and Testimonials 16 CFR Part 465, 22 August 2024, available at: https://www.federalregister.gov/documents/2024/08/22/2024-18519/trade-regulation-rule-on-the-use-of-consumer-reviews-and-testimonials.
- US Financial Crimes Enforcement Network, FinCEN Advisory FIN-2017-A007 (2017), available at: https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017-a007-0.
- US Food and Drug Administration, 6 Tip-offs to Rip-offs: Don't Fall for Health Fraud Scams (2021), available at: https://www.fda.gov/consumers/consumer-updates/6-tip-offs-rip-offs-dont-fall-health-fraud-scams.
- US Food and Drug Administration, Warning Letter (2024), available at: https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/amazoncom-inc-679523-07252024
- US National Institute of Standards and Technology (NIST), Reducing Risks Posed by Synthetic Content: An Overview of Technical Approaches to Digital Content Transparency (2024), available at: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-4.pdf
- US Securities and Exchange Commission, Risky Business: "Pre-IPO" Investing (2005), available at: https://www.sec.gov/about/reports-publications/investorpubspreipohtm
- Singapore Ministry of Home Affairs, Assessment of Carousell's and Meta's Enhanced Verification Measures Under the E-commerce Code of the Online Criminal Harms Act (2025), available at: https://www.mha.gov.sg/media-room/newsroom/assessment-of-carousell-and-meta-enhanced-verification-measures-under-the-e-commerce-code-of-the-online-criminal-harms-act/.
- Singapore Ministry of Home Affairs, Enhanced Verification Measures by Carousell Under the E-Commerce Code of the Online Criminal Harms Act (2025), available at: https://www.mha.gov.sg/media-room/newsroom/enhanced-verification-measures-by-carousell-under-the-e-commerce-code-of-the-online-criminal-harms-act/
- Singapore Ministry of Home Affairs, Status of step-up measures to be implemented by Carousell and additional consumer protection measures against

e-commerce scams (2026), available at: https://www.mha.gov.sg/media-room/newsroom/status-of-step-up-measures-to-be-implemented-by-carousell-and-additional-consumer-protection-measures-against-e-commerce-scams/
- Taiwan Ministry of the Interior, Fraud Crime Hazard Prevention Act, available at: https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=D0080226.

Consumer Organisations / Civil Society Organisations
- AI Forensics, AI-generated Algorithmic Virality (2025), available at: https://aiforensics.org/uploads/GenAI%20Report.pdf
- AI Forensics, No Embargo in Sight (2025), available at: https://aiforensics.org/uploads/No_Embargo_in_Sight_AI_Forensics_Report.pdf
- AI Forensics, Meta Ads: A Pill Hard to Swallow (2024), available at: https://aiforensics.org/uploads/meta_health.pdf
- AI Forensics, Meta's Failing Ad Moderation: Health Scams Targeting EU Users (2025), available at: https://aiforensics.org/work/meta-health-ads
- AI Forensics, TikTok's Research API: Problems without Explanations (2025), available at: https://arxiv.org/pdf/2506.09746
- Altroconsumo, Prenotazioni su Booking.com: occhio alla truffa del sito clone (2025), available at: https://www.altroconsumo.it/soldi/truffe/news/truffa-sito-booking-clone
- Banking & Payments Federation Ireland, Almost €9.4m laundered through money mule accounts (2025), available at: https://bpfi.ie/money-mules-2025/
- BDO / Fraud Advisory Panel, Charity Fraud Report: a five-year review (2026), available at: https://www.bdo.co.uk/getmedia/622cc7e5-f5fc-4bf3-87bc-f92dfffb95e4/NFP-Report-BDO-Charity-Fraud-Report-2025.pdf
- BEUC, Digital Services Act should help consumers online but success depends on strong enforcement (2022), available at: https://www.beuc.eu/press-releases/digital-services-act-should-help-consumers-online-success-depends-strong-enforcement
- BEUC, Free, easy and secure – What consumers expect from the digital euro (2025), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-085_What_consumers_expect_from_the_digital_euro-copy.pdf
- BEUC, Turning Stars into Trust: How to make online reviews more reliable (2025), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-027_how_to_make_online_reviews_more_reliable.pdf
- BEUC, Hype or Harm? The Great Social Media Crypto Con (2023), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2023-073_Hype_or_harm_The_great_social_media_crypto_con.pdf
- BEUC, Sponsored by Scammers: How Big Tech Platforms Facilitate Financial Fraud (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf
- BEUC, Under the Microscope: Tests of Temu Products by Consumer Groups (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2025-007_Tests_of_Temu_Products_by_Consumer_Groups.pdf

- BEUC, Unsafe and Illegal Activities Online, available at: https://www.beuc.eu/sites/default/files/publications/unsafe_and_illegal_activities_online.pdf.
- ECC-Net, The impact of counterfeiting on online consumer rights in Europe (2017), available at: https://www.eccbelgium.be/brochures/detail/ecc-net-report-the-impact-of-counterfeiting-on-online-consumer-rights-in-europe
- ECC-Net, Fraud in Cross-border E-commerce (2016), available at: https://www.eccnet.eu/publication/online-fraud
- Euroconsumers, Caught in the web: Navigating the digital maze of scams (2024), available at: https://www.euroconsumers.org/wp-content/uploads/2024/12/Caught-in-the-web-Navigating-the-digital-maze-of-scams.pdf
- Euroconsumers, Form fraud is rife on booking.com: Your scam stories can help to stop criminals (2025), available at: https://www.euroconsumers.org/fraud-booking-com-share-scam-stories/
- FEAT, 1750 Potentially Fraudulent Tickets Offered for Radiohead's European Tour (2025), available at: https://www.feat-alliance.org/2025/09/17/1750-potentially-fraudulent-tickets-offered-for-radioheads-european-tour/
- Febelfin, Chiffres 2024: 'Si ça ressemble à du phishing, c'est probablement du phishing !' (2025), available at: https://febelfin.be/fr/themes/fraude-et-securite/chiffres-et-tendances/chiffres-2024-si-ca-ressemble-a-du-phishing-c-est-probablement-du-phishing
- Febelfin, Phishing & autres arnaques en vue (2024), available at: https://febelfin.be/media/pages/publicaties/2024/phishing-en-andere-kapers-op-de-kust/48633be3fd-1718872012/storytelling_phishing_fr_final.pdf
- National Center for Missing & Exploited Children, Generative AI (GAI) (n.d.), available at: https://www.missingkids.org/theissues/generative-ai
- Taenk, Digital svindel i Danmark - En undersøgelse af danskernes holdninger, erfaringer og adfærd (2025), available at: https://taenk.dk/system/files?file=2025-05/Digital%20svindel%20i%20Danmark_FINAL_290425.pdf
- UNIFAB (Union des Fabricants), Counterfeiting & Organised Crime (2025), available at: https://www.unifab.com/wp-content/uploads/2025/06/UNIFAB_Contrefacon-Criminalite_ENGLISH_VDEF_03062025.pdf
- SWGfL, Revenge Porn Helpline 2022 Annual Report (2022), available at: https://swgfl.org.uk/research/revenge-porn-helpline-2022-report/
- Watchlist Internet, Die Evolution des Online-Betrugs: Vom klassischen Internetbetrug zur KI-gestützten Täuschung (2024), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Bericht_KI_und_Betrug_final.pdf
- Watchlist Internet, Das können Sie tun, wenn Kriminelle Ihren Online-Shop kopieren, available at: https://www.watchlist-internet.at/news/das-koennen-sie-tun-wenn-kriminelle-ihren-online-shop-kopieren/
- Watchlist Internet, "Liste betrügerischer Online-Shops," available at: https://www.watchlist-internet.at/liste-betruegerischer-shops
- Watchlist Internet, Massenhaft irreführende Werbung von problematischen Online-Shops auf Facebook und Instagram (2025), available at:

https://www.watchlist-internet.at/news/irrefuehrende-werbung-auf-meta-plattformen/
- Watchlist Internet, Promis als Lockvögel: Werbung für betrügerische Investmentplattformen erreicht täglich 200.000 Österreicher:innen (2024), available at: https://www.watchlist-internet.at/news/werbung-promis-investmentbetrug/
- Watchlist Internet, Trends und Entwicklungen bei Fake-Shops, available at: https://www.watchlist-internet.at/news/trends-und-entwicklungen-bei-fake-shops/
- Watchlist Internet, Vorsicht vor Werbung unseriöser Online-Shops!, available at: https://www.watchlist-internet.at/news/vorsicht-vor-werbung-unserioeser-online-shops/.
- Watchlist Internet, "Wege in Fake-Shops," available at: https://www.watchlist-internet.at/news/wege-in-fake-shops/
- WeProtect Global Alliance, A web of deceit: financial sexual extortion of children and young people (2024), available at: https://www.weprotect.org/resources/library/financial-sexual-extortion-of-children-and-young-people/
- What To Fix, Systemic Risks – Social Media Monetization Systems: A Risk Factor (2025), available at: https://drive.google.com/file/d/1UeKYU3qyeOfEY--oz2hovSpAtx-upOoD/view
- Which?, The psychology of scams, Understanding why consumers fall for APP scams (2022), available at: https://media.product.which.co.uk/prod/files/file/gm-c66f3d70-3928-4dee-bb8b-481405be2b5e-the-psychology-of-scams-understanding-why-consumers-fall-for-app-scams.pdf
- Which?, The scam crisis on Booking.com (2025), available at: https://www.which.co.uk/news/article/the-scam-crisis-on-booking.com-aAj2P4i2c06f
- Which?, What went wrong with Booking.com? (2025), available at: https://www.which.co.uk/news/article/what-went-wrong-with-booking.com-aYOyv4Q7Ua2D.

Trusted Flagger Reports

- AK Wien and ÖIAT, #KEINEWERBUNG? Schleichwerbung und problematische Marketingkommunikation auf TikTok (2025), available at: https://wien.arbeiterkammer.at/beratung/konsumentenschutz/achtungfalle/Schleichwerbung_auf_Tiktok_202505.pdf
- Debunk, Debunk.org Trusted Flagger 2025 Report (2026), available at: https://www.debunk.org/debunk-org-trusted-flagger-2025-report
- FactReview, Special Trusted Flagger Report #1 (2025), available at: https://factreview.gr/2025/01/31/trusted-flagger-special-report-1-eng/
- FactReview, Trusted Flagger Report #2 (2026), available at: https://factreview.gr/2026/03/03/trusted-flagger-report-2-en/
- ÖIAT/AIT, Fake-Shop Detector, available at: https://research.oiat.at/fake-shop-detector

- ÖIAT, Verbreitung von Abo-Fallen durch Google Ads (2026), available at: https://www.watchlist-internet.at/fileadmin/files/Abo-Fallen/Google-Policy-Paper.pdf
- ÖIAT, Dubiose Werbung auf Meta-Plattformen: Wie Celebrity-Ärzte zur Bewerbung von Nahrungsergänzungsmitteln missbraucht werden (2025), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Safe-NEM-Bericht.pdf
- ÖIAT, Numerous fraudulent ghost stores on Facebook and Instagram (2025), available at: https://research.ÖIAT.at/fileadmin/Research/Dokumente/Ghost_Stores_Erhebung_en.pdf
- ÖIAT, FraudSeeker Report (2024), available at: https://research.oiat.at/fileadmin/Research/Dokumente/netidee_Call17_FraudSeeker_Studienbericht.pdf
- Verbraucherzentrale Bundesverband, Jeder zweite Fakeshop schaltet Werbung auf Google oder Meta (2025), available at: https://www.vzbv.de/pressemitteilungen/jeder-zweite-fakeshop-schaltet-werbung-auf-google-oder-meta
- Verbraucherzentrale Bundesverband, Bank Oder Betrüger? Erhebung zur Erkennbarkeit von Betrug im digitalen Zahlungsverkehr (2024), available at: https://www.vzbv.de/sites/default/files/2024-05/24-05-09%20Bericht_vzbv_Betrugserkennung.pdf

Academic Articles

- Acharya, B. and Holz, T., An Explorative Study of Pig Butchering Scams (2024), available at: https://arxiv.org/pdf/2412.15423
- Adamopoulos, P., The Spillover Effect of Fraudulent Reviews on Product Recommendations (2024), available at: https://dl.acm.org/doi/10.1287/mnsc.2021.02612
- Aidoo, S., Customer Due Diligence (CDD) and Know Your Customer (KYC) (2025), available at: https://www.researchgate.net/profile/Samuel-Aidoo-2/publication/393884914_Customer_Due_Diligence_CDD_and_Know_Your_Customer_KYC
- Akhawe D and Porter Felt A, Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness (2013), available at: https://www.usenix.org/conference/usenixsecurity13/technical-sessions/presentation/akhawe.
- Al-Hamad E.A. et al., Reporting Social Media Fraud: Motivations, Barriers, and Reporting Mechanism, in Mahmoud Barhamgi et al. (eds), Web Information Systems Engineering (2024), available at: https://doi.org/10.1007/978-981-96-0570-5_29.
- Anderson, M. et al., Exploring the roles played by trust and technology in the online investment fraud victimisation process (2024), available at: https://journals.sagepub.com/doi/pdf/10.1177/26338076241248176
- Assenmacher, D. et al., Demystifying Social Bots: On the Intelligence of Automated Social Media Actors (2020), available at: https://journals.sagepub.com/doi/pdf/10.1177/2056305120939264

- Balcombe, L., The mental health impacts of internet scams (2025), available at: https://www.mdpi.com/1660-4601/22/6/938
- Bartoletti, M. et al., Cryptocurrency Scams: Analysis and Perspectives (2021), available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9591634
- Bartuzi-Trokielewicz E and Martinek A, Anatomy of Generative Scam Campaigns in Online Advertising Ecosystems (2026), available at: https://dl.acm.org/doi/pdf/10.1145/3774905.3794690
- Bekkers, L.M.J. and Leukfeldt, E.R., Recruiting money mules on Instagram: a qualitative examination of the online involvement mechanisms of cybercrime (2022), available at: https://www.tandfonline.com/doi/full/10.1080/01639625.2022.2073298
- Bevendorff, J. et al., Is Google Getting Worse? A Longitudinal Investigation of SEO Spam in Search Engines (2024), available at: https://downloads.webis.de/publications/papers/bevendorff_2024a.pdf
- Bhattacharya S and Singh A, Unravelling the Infodemic: A Systematic Review of Misinformation Dynamics During the COVID-19 Pandemic (2025), available at: https://www.frontiersin.org/journals/communication/articles/10.3389/fcomm.2025.1560936/full
- Bilz, A. et al., Tainted Love: a Systematic Literature Review of Online Romance Scam Research (2023), available at: https://academic.oup.com/iwc/article/35/6/773/7331428
- Bondi, T. and Rossi, M., Online Reviews: Information Content, Drivers, and Platform Design (2026), available at: https://www.ifo.de/DocDL/cesifo1_wp12427.pdf
- Burton SL and Moore PD, Pig Butchering in Cybersecurity: A Modern Social Engineering Threat (2024), available at: https://commons.erau.edu/publication/2266.
- Chergarova, V. et al., Cryptocurrency fraud: A study on the characteristics of criminals who are using fake profiles on a social media platform to persuade individuals to invest into cryptocurrency (2022), available at: https://iacis.org/iis/2022/3_iis_2022_242-252.pdf
- Chu, A. et al., Behind the Tube: Exploitative Monetization of Content on YouTube (2022), available at: https://www.usenix.org/system/files/sec22-chu.pdf
- Chuai Y et al, From News Source Sharers to Post Viewers: How Topic Diversity and Conspiracy Theories Shape Engagement With Misinformation During a Health Crisis (2024), available at: https://arxiv.org/pdf/2401.08832.
- Chen R et al., An Analysis of the Factors Influencing Engagement Metrics Within the Dissemination of Health Science Misinformation (2025), available at: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC12180413/.
- Cross, C., Romance baiting, cryptorom and 'pig butchering': an evolutionary step in romance fraud (2024), available at: https://www.tandfonline.com/doi/pdf/10.1080/10345329.2023.2248670
- Cross, C. and Holt, K., To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud (2023), available at: https://journals.sagepub.com/doi/pdf/10.1177/17488958221149581
- Cross, C. and Grant-Smith, D., Recruitment Fraud: Increased opportunities for exploitation in times of uncertainty? (2022), available at:

https://socialalternatives.com/wp-content/uploads/2022/02/CrossGrant-Smith-SA40-4.pdf

- DeLiema, M., Profiling Victims of Investment Fraud: Mindsets and Risky Behaviors (2019), available at: https://academic.oup.com/jcr/article-abstract/46/5/904/5512363
- Devi P et al., Influencer or Finfluencer: A Comprehensive Study of Behavioural Financial in the Age of Digital Social Media (2026), available at: https://ieeexplore.ieee.org/abstract/document/11465570
- Drew, J.M. and Webster, J., The victimology of online fraud: A focus on romance fraud victimisation (2024), available at: https://www.sciencedirect.com/science/article/pii/S2949791424000058
- Dulisse, B. et al., Old techniques, new technologies: Exploring patterns from scammers that commit financial fraud via cryptocurrency (2025), available at: https://www.sciencedirect.com/science/article/pii/S2949791425000545
- Edwards, M., Online sextortion: Characteristics of offences from a decade of community reporting (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000386
- Egelman S, Cranor LF and Hong J, You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings (2008), available at: https://doi.org/10.1145/1357054.1357219
- Esoimeme, E.E., Identifying and reducing the money laundering risks posed by individuals who have been unknowingly recruited as money mules (2021), available at: https://www.emerald.com/jmlc/article-abstract/24/1/201/241861/Identifying-and-reducing-the-money-laundering
- Faux, Z, Number go up: Inside Crypto's wild rise and staggering fall (2024, Penguin Random House)Feeney, A.J. et al., Global perspective of the risks of falsified and counterfeit medicines: A critical review of the literature (2024), available at: https://www.sciencedirect.com/science/article/pii/S1477893924000759
- Herke C and Szabo B, Artificial Intelligence and Crime on Social Media Platforms (2026), available at: https://www.intechopen.com/online-first/1249383.
- Hong, G. et al., Analyzing Ground-Truth Data of Mobile Gambling Scams (2022), available at: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=9833665
- Kassem, R. and Carter, E., Mapping romance fraud research – a systematic review (2024), available at: https://www.emerald.com/jfc/article-abstract/31/4/974/1238258/Mapping-romance-fraud-research-a-systematic-review
- Khachatryan, A., The Digital Dilemma: Counterfeit Culture and Brand Protection Reform in the E-Commerce Era (2023), available at: https://digitalcommons.lmu.edu/cgi/viewcontent.cgi?article=1659&context=elr
- Kieffer, C.N. and Mottola, G.R., Understanding and Combating Investment Fraud (2016), available at: https://pensionresearchcouncil.wharton.upenn.edu/wp-content/uploads/2017/02/WP2016-19-Kieffer-and-Mottola.pdf
- Kipngetich, A., A review of online scams and financial frauds in the digital age (2025), available at:

https://gsconlinepress.com/journals/gscarr/sites/default/files/GSCARR-2025-0025.pdf

- Kisa A and Kisa S, Health Conspiracy Theories: A Scoping Review of Drivers, Impacts, and Countermeasures (2025), available at: https://link.springer.com/article/10.1186/s12939-025-02451-0
- Kotzias, P. et al., Scamdog Millionaire: Detecting E-commerce Scams in the Wild (2023), available at: https://dl.acm.org/doi/pdf/10.1145/3627106.3627184
- Lazarus, S. et al., What do we know about online romance fraud studies? A systematic review of the empirical literature (2000 to 2021) (2023), available at: https://www.sciencedirect.com/science/article/pii/S2949791423000131
- Lee, S. et al., Fraud Detection on Crowdfunding Platforms Using Multiple Feature Selection Methods (2025), available at: https://xplorestaging.ieee.org/ielx8/6287639/10820123/10909102.pdf
- Lee, S, Detecting Bias in Machine Learning Models (2025), available at: https://www.numberanalytics.com/blog/ultimate-guide-bias-detection-machine-learning.
- Lee Y et al., Understanding iOS-based Crowdturfing Through Hidden UI Analysis (2019), available at: https://par.nsf.gov/servlets/purl/10172762.
- Leukfeldt, E.R., Cybercrime and social ties. Phishing in Amsterdam (2014), available at: https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/trndorgc17&section=22
- Levi, M., Frauds and Their Controls: Some Scholarly Reflections (2025), available at: https://www.journals.uchicago.edu/doi/10.1086/736347
- Li, X. et al., Double and Nothing: Understanding and Detecting Cryptocurrency Giveaway Scams (2023), available at: https://www.ndss-symposium.org/wp-content/uploads/2023/02/ndss2023_f584_paper.pdf
- Lim, A. and Choi, K., Modus operandi and blockchain analysis of romance scams: Cryptocurrency-driven victimization (2025), available at: https://vc.bridgew.edu/cgi/viewcontent.cgi?article=1220&context=ijcic
- Liu, E. et al., Give and Take: An End-To-End Investigation of Giveaway Scam Conversion Rates (2024), available at: https://arxiv.org/pdf/2405.09757
- Luoma-aho, V. et al., Vulnerabilities to Crypto Currency Scams and Online Persuasion Strategies (2025), available at: https://jyx.jyu.fi/bitstreams/5459bc01-0ded-457b-b4ab-45617cbecc08/download
- Mahbub, S. and Pardede, E., Using Contextual Features for Online Recruitment Fraud Detection (2018), available at: https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1247&context=isd2014
- Mangiò F and Di Domenico G, All that Glitters Is Not Real Affiliation: How to Handle Affiliate Marketing Programs in the Era of Falsity (2022), available at: https://www.sciencedirect.com/science/article/pii/S0007681322000775.
- Marciel M et al., Understanding the Detection of View Fraud in Video Content Portals (2016), available at: https://arxiv.org/pdf/1507.08874.
- Mölders M, et al., Understanding Finfluencers: Roles and Strategic Partnerships in Retail Investor Engagement (2025), available at: https://www.sciencedirect.com/science/article/pii/S0148296325002851.

- Nasir, W., Cryptocurrency Fraud and Financial Crime: Analyzing Convicted Fraudsters in Digital Asset Scams (2025), available at: https://www.authorea.com/doi/full/10.22541/au.174180456.65670202
- Nasir, W. and Ali, K., Online Romance Scams and Digital Asset Fraud: Investigating Cross-Border Criminal Networks (2025), available at: https://www.researchgate.net/profile/Khalid-Ali-56/publication/389991094_Online_Romance_Scams_and_Digital_Asset_Fraud_Investigating_Cross-Border_Criminal_Networks
- Newall P.W.S, What Is Sludge? Comparing Sunstein's Definition to Others (2023), available at: https://research-information.bris.ac.uk/ws/portalfiles/portal/321458464/Review_of_sludge_Newall.pdf.
- Niu, J et al., A survey on membership inference attacks and defenses in machine learning (2024), available at: https://www.sciencedirect.com/science/article/pii/S2949715924000064
- Oak, R. and Shafiq, Z., "Hello, is this Anna?": Unpacking the Lifecycle of Pig-Butchering Scams (2025), available at: https://www.usenix.org/system/files/soups2025-oak-butchering.pdf
- Papasavva, A. et al., Applications of AI-Based Models for Online Fraud Detection and Analysis (2025), available at: https://link.springer.com/content/pdf/10.1186/s40163-025-00248-8.pdf
- Pava, M. et al., Mind the (Language) Gap: Mapping the Challenges of LLM Development in Low-Resource Language Contexts (2025), available at: https://hai.stanford.edu/policy/mind-the-language-gap-mapping-the-challenges-of-llm-development-in-low-resource-language-contexts
- Pflücke F, Europe's Fragmented Approach to Finfluencer Regulation: Post #4 for the Blogposium on Finfluencers (2026), available at: https://corporatelawacademic.wordpress.com/2026/01/30/europes-fragmented-approach-to-finfluencer-regulation-post-4-for-the-blogposium-on-finfluencers/.
- Pflücke F, Regulating Influencers in the European Union: Current Challenges and Future Perspectives (2024), available at: https://www.cecluxembourg.lu/wp-content/uploads/5-Pflucke_influencers.pdf
- Policastro, C. and Payne, B.K., Can you hear me now? Telemarketing fraud victimisation and lifestyles (2015), available at: https://www.researchgate.net/publication/280973645_Can_You_Hear_Me_Now_Telemarketing_Fraud_Victimization_and_Lifestyles
- Putta, S. et al., Machine Learning Approach for Fake Job Ad Prediction (2023), available at: https://www.proquest.com/openview/00c88ab1a6b7334de114d32519cfae08/1
- Raj, A. et al., Counterfeit medicine: a major public health concern and effective remedies for combatting the crisis (2025), available at: https://link.springer.com/article/10.1007/s44395-025-00004-6
- Rani, M.I.A. et al., Exploring Money Mule Recruitment: An Initiative in Combating Money Laundering (2023), available at: https://www.researchgate.net/profile/Salwa-Zolkaflil/publication/369823521_EXPLORING_MONEY_MULE_RECRUITMENT_AN_INITIATIVE_IN_COMBATING_MONEY_LAUNDERING

- Ravanelle, A.J. et al., Good jobs, scam jobs: Detecting, normalizing, and internalizing online job scams during the COVID-19 pandemic (2022), available at: https://journals.sagepub.com/doi/pdf/10.1177/14614448221099223
- Raza, M.S. et al., Role of money mules in money laundering and financial crimes (2020), available at: https://ideas.repec.org/a/eme/jfcpps/jfc-02-2020-0028.html
- Reid, J., Delusive speech in the sharing economy: Scam Inc. (2025), available at: https://www.taylorfrancis.com/books/mono/10.4324/9781003513995/delusive-speech-sharing-economy-julie-reid
- Rössler A, et al.,, FaceForensics++: Learning to Detect Manipulated Facial Images (2019), available at: https://www.researchgate.net/publication/330672957_FaceForensics_Learning_to_Detect_Manipulated_Facial_Images.
- Saad, M.E., Cyber Romance Scam Victimization Analysis using Routine Activity Theory Versus Apriori Algorithm (2018), available at: https://www.proquest.com/openview/8b75a9c1d7acab599b654754d2482c26/1
- Saberi M et al., Robustness of AI-Image Detectors: Fundamental Limits and Practical Attacks (2024), available at: https://arxiv.org/pdf/2310.00076
- Schokkenbroek, J.M. and Snaphaan, T., Love as Bait: A Scoping Review and Crime Script Analysis of Online Romance Scams (2025), available at: https://journals.sagepub.com/doi/full/10.1177/15248380251361046
- Sen A, Influence of Social Media and Finfluencers on Investor Behaviour (2026), available at: https://www.ijfmr.com/papers/2026/1/66685.pdf
- Sheil, A. et al., Staying at the Roach Motel: Cross-Country Analysis of Manipulative Subscription and Cancellation Flows (2024), available at: https://arxiv.org/pdf/2309.17145
- Shepherd, D. et al., The Impact of Deviant Social Media Influencers and Consumer Characteristics on Purchasing Counterfeit Goods (2023), available at: https://www.tandfonline.com/doi/epdf/10.1080/01639625.2023.2233041
- Shimamura, M., Uncovering Black-hat SEO based fake E-commerce scam groups from their redirectors and websites (2025), available at: https://arxiv.org/html/2505.21021v1
- Singh K and Zou J, New Evaluation Metrics Capture Quality Degradation due to LLM Watermarking (2023), available at: https://arxiv.org/pdf/2312.02382
- Srivani, P. et al., Machine Learning Approach for Fake Job Ad Prediction (2023), available at: https://www.proquest.com/openview/00c88ab1a6b7334de114d32519cfae08/1
- Sunstein, C.R., Sludge and Ordeals (2019), available at: https://scholarship.law.duke.edu/dlj/vol68/iss8/6/.
- Szymielewicz, K., Reclaiming the Algorithm: What the DSA can–and can't–fix about recommender systems (2026), available at: https://dsa-observatory.eu/2026/02/15/reclaiming-the-algorithm-what-the-dsa-can-and-cant-fix-about-recommender-systems/
- Tavabi, N. et al., Characterizing Activity on the Deep and Dark Web (2019), available at: https://dl.acm.org/doi/pdf/10.1145/3308560.3316502
- Thaler,R.H. and Sunstein, C.R., Nudge: Improving Decisions About Health, Wealth and Happiness (2008), available at:

https://www.researchgate.net/file.PostFileLoader.html?id=53abe564cf57d7df1e8b45f4&assetKey=AS%3A273548994646025%401442230571326

- Tomasena JM, et al., Networking and monetization strategies of Spanish-speaking finfluencers: a co-link analysis of YouTube descriptions (2025), available at: https://spir.aoir.org/ojs/index.php/spir/article/view/15343
- Urosevic D et al., Countering Technical Support Scams (2019), available at: https://www.microsoft.com/en-us/research/wp-content/uploads/2018/12/CounterTechSupportScams.pdf.
- Tran Truong B et al., Audit of takedown delays across social media reveals failure to reduce exposure to illegal content (2026), available at: https://arxiv.org/html/2502.08841v3
- University of Cambridge, Cambridge Online Trust and Safety Index, available at: https://cotsi.org/platforms?view=map&platform=ig
- Van Der Zee, S. et al., The gift of the gab: Are rental scammers skilled at the art of persuasion? (2019), available at: https://arxiv.org/abs/1911.08253
- Vance A et al., Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments (2018), available at: https://www.jstor.org/stable/26630238.
- Vardhan, R. et al., #DM-Me: Susceptibility to Direct Messaging-Based Scams (2023), available at: https://dl.acm.org/doi/pdf/10.1145/3579856.3582815
- Wang, F., A scoping review of online romance scams: Conceptual construction and comparative analysis (2026), available at: https://journals.sagepub.com/doi/pdf/10.1177/02697580251414141
- Wang, F. and Topalli, V., The Cyber-Industrialization of Catfishing and Romance Fraud (2023), available at: https://www.sciencedirect.com/science/article/pii/S0747563223004843
- Wang L et al., From Inquisitorial to Adversarial: Using Legal Theory to Redesign Reporting Systems in Online Communities (2026), available at: https://arxiv.org/pdf/2506.07041
- Wardle, H. and Zendle, D., Loot Boxes, Gambling, and Problem Gambling Among Young People (2021), available at: https://journals.sagepub.com/doi/pdf/10.1089/cyber.2020.0299
- Whitty, M., A systematic literature review of profiling victims of cyber scams: setting up a framework for future research (2025), available at: https://www.tandfonline.com/doi/pdf/10.1080/23311886.2025.2563781
- Whitty, M., Is There a Scam for Everyone? Psychologically Profiling Cyberscam Victims (2020), available at: https://link.springer.com/article/10.1007/s10610-020-09458-z
- Whitty, M., Do You Love Me? Psychological Characteristics of Romance Scam Victims (2018), available at: https://journals.sagepub.com/doi/full/10.1089/cyber.2016.0729
- Whitty, M., The online dating romance scam: The psychological impact on victims – both financial and non-financial (2015), available at: https://journals.sagepub.com/doi/abs/10.1177/1748895815603773
- Wilcox, H. and Bhattacharya, M., A human dimension of hacking: Social engineering through social media (2020), available at: https://arxiv.org/pdf/2005.04049

- Wittenberg C et al., Labeling AI-Generated Content: Promises, Perils, and Future Directions (2023), available at: https://computing.mit.edu/wp-content/uploads/2023/11/AI-Policy_Labeling.pdf
- Xiao, J., Xiao, Q. and Shen, H., "It felt real": victim perspectives on platform design and longer-running scams (2025), available at: https://arxiv.org/pdf/2510.02680
- Zhao Y et al., No Source Code? No Problem! Demystifying and Detecting Mask Apps in iOS (2024), available at: https://dl.acm.org/doi/pdf/10.1145/3643916.3644419.
- Zülch H, Mölders M and Hoffmann CP, Navigating the rise of finfluencers: a multidimensional quality framework for strategic partnerships (2025), available at: https://www.econstor.eu/bitstream/10419/338848/1/41264_2025_Article_334.pdf.

News Articles

- Business Insider, A Chinese criminal ring has stolen $50 million by franchising thousands of fake online shops (2024), available at: https://www.businessinsider.com/fake-online-shops-china-crime-ring-franchise-model-target-americans-2024-5
- CNBC, On #GivingTuesday, check into that crowdfunding campaign before you donate (2018), available at: https://www.cnbc.com/2018/11/27/how-to-avoid-fraud-on-crowdfunding-sites.html.
- Consumer Reports, Hijacked Reviews on Amazon Can Trick Shoppers (2019), available at: https://www.consumerreports.org/customer-reviews-ratings/hijacked-reviews-on-amazon-can-trick-shoppers/.
- Demagog, Metoda "na walizkę" – jak działają oszuści na Facebooku? (2024), available at: https://demagog.org.pl/analizy_i_raporty/jak-oszusci-z-cypru-okradaja-polakow-oto-historia-pani-iwony/
- Euronews, Behind the global scam worth an estimated €100m targeting WhatsApp users with fake job offers (2023), available at: https://www.euronews.com/next/2023/10/23/behind-the-global-scam-worth-an-estimated-100m-targeting-whatsapp-users-with-fake-job-offe
- EUobserver, Google's AI search feature raises concerns over scams and misinformation (2025), available at: https://euobserver.com/digital/aradc7eaf8.
- Franceinfo, Paris 2024 : 338 sites internet frauduleux de revente de billets recensés à quelques semaines du début de la compétition (2024), available at: https://www.franceinfo.fr/les-jeux-olympiques/paris-2024/info-franceinfo-paris-2024-338-sites-internet-frauduleux-de-revente-de-billets-recenses-a-quelques-semaines-du-debut-de-la-competition_6543401.html
- Forbes, Job Seekers: Be Careful Using LinkedIn's New "Open To Work" Feature (2020), available at: https://www.forbes.com/sites/roberthellmann/2020/07/20/job-seekers-be-careful-using-linkedins-new-open-to-work-feature
- Investigate Europe, Scam Europe (2025), available at: https://www.investigate-europe.eu/themes/investigations/-scam-europe

- Investigate Europe, The rogue 'finfluencers' pushing risky investments to young followers (2025), available at: https://www.investigate-europe.eu/posts/the-rogue-finfluencers-pushing-risky-investments-to-young-followers
- Levanta la cabeza, El fraude digital aumenta un 40% en España: 1.200 estafas al día en 2025 (2025), available at: https://www.atresmedia.com/levanta-la-cabeza/buenas-practicas/ciberseguridad/fraude-digital-aumenta-40-espana-1200-estafas-dia-2025_202512306953a7ee22f0db7daf011949.html
- Reuters, EU regulator flags surge in online sales of counterfeit weight-loss drugs (2025), available at: https://www.reuters.com/sustainability/boards-policy-regulation/eu-regulator-flags-surge-online-sales-counterfeit-weight-loss-drugs-2025-09-03/
- Reuters, Meta created 'playbook' to fend off pressure to crack down on scammers, documents show (2026), available at: https://www.reuters.com/investigations/meta-created-playbook-fend-off-pressure-crack-down-scammers-documents-show-2025-12-31/
- Reuters, Meta is earning a fortune on a deluge of fraudulent ads, documents show (2025), available at: https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/
- RTBF, Les signalements de fraude aux tickets de concerts ont doublé en un an (2024), available at: https://www.rtbf.be/article/les-signalements-de-fraude-aux-tickets-de-concerts-ont-double-en-un-an-j-ai-perdu-180-et-je-n-ai-jamais-recu-mes-places-11394129
- RTE, One third of social media users targeted by fake adverts (2024), available at: https://www.rte.ie/news/business/2024/1115/1481149-one-third-of-social-media-users-targeted-by-fake-adverts/
- TechBuzz, Meta deploys AI scam detection across all platforms (2026), available at: https://www.techbuzz.ai/articles/meta-deploys-ai-scam-detection-across-all-platforms
- The Guardian, 'Ghost broking': cut-price car insurance isn't all it seems (2025), available at: https://www.theguardian.com/money/2025/nov/16/ghost-broking-cut-price-car-insurance-scam-watch
- The Guardian, 'Money mule' cases surge as criminals target young people on social media (2025), available at: https://www.theguardian.com/money/2025/dec/22/money-mule-cases-surge-as-criminals-target-young-people-on-social-media
- The Hacker News, AI-Driven Pushpaganda Scam Exploits Google Discover to Spread Scareware and Ad Fraud (2026), available at: https://thehackernews.com/2026/04/ai-driven-pushpaganda-scam-exploits.html.
- The Wall Street Journal, Meta Battles an 'Epidemic of Scams' as Criminals Flood Instagram and Facebook (2025), available at: https://www.wsj.com/tech/meta-fraud-facebook-instagram-813363c8
- TorrentFreak, Share With Care: 2,217 Domains Blocked, The Majority For Circumvention (2024), available at: https://torrentfreak.com/share-with-care-2217-pirate-domains-blocked-most-for-circumventing-blocking-240114/
- TorrentFreak, Google Sees DMCA Takedown Requests Surge to New Highs (2024), available at: https://torrentfreak.com/google-sees-dmca-takedown-requests-surge-to-new-highs-240110/

- TorrentFreak, Google Search Processed a Billion DMCA Takedowns in Four Months (2024), available at: https://torrentfreak.com/google-search-processed-a-billion-dmca-takedowns-in-four-months-240622/
- TorrentFreak, Google Asked to Remove 10 Billion "Pirate" Search Results (2024), available at: https://torrentfreak.com/google-asked-to-remove-10-billion-pirate-search-results-241105/
- VICE, Scammers Are Sending Fake Job Offers on LinkedIn (2021), available at: https://www.vice.com/en/article/scammers-are-sending-fake-job-offers-on-linkedin/
- VICE, Those 'DM to Collab' Instagram Messages Are Probably a Scam (2021), available at: https://www.vice.com/en/article/dm-to-collab-instagram-messages-scam/
- VRT, Youngsters don't realise the risk of becoming a money mule (2022), available at: https://www.vrt.be/vrtnws/en/2022/11/29/_youngsters-don_t-realise-the-risk-of-becoming-a-money-mule/
- WIRED, Elon Musk's Twitter Is a Scammer's Paradise (2022), available at: https://www.wired.com/story/twitter-blue-check-verification-buy-scams/.
- WIRED, Malicious Ads in Search Results Are Driving New Generations of Scams (2024), available at: https://www.wired.com/story/malicious-ads-in-search-results-are-driving-new-generations-of-scams.

Industry Reports

- AppleInsider, App Store scams are getting worse and Apple isn't doing enough (2026), available at: https://appleinsider.com/articles/26/04/17/app-store-scams-are-getting-worse-and-apple-isnt-doing-enough
- AppleInsider, Bogus crypto wallet on App Store steals $9.5M (2026), available at: https://appleinsider.com/articles/26/04/14/bogus-crypto-wallet-on-app-store-steals-95m
- Better Finance, Unmasking Digital Deception: A Data-Driven Approach to Mapping and Combating Online Investment Fraud in Europe (2024), available at: https://betterfinance.eu/publication/unmasking-digital-deception-a-data-driven-approach-to-mapping-and-combating-online-investment-fraud-in-europe/
- BioCatch, Germans lose €267 billion to cybercrime (2025), available at: https://www.biocatch.com/press-release/germans-lose-267-billion-to-cybercrime
- Bitdefender, Action Fraud Urges Vigilance as Ticket Fraud Losses Surge to £9.7 Million (2025), available at: https://www.bitdefender.com/en-gb/blog/hotforsecurity/action-fraud-urges-vigilance-as-ticket-fraud-losses-surge-to-9-7-million
- Bitdefender, Metallica and The Weeknd Fans Targeted in Fake Concert Ticket Scams (2025), available at: https://www.bitdefender.com/en-us/blog/hotforsecurity/metallica-and-the-weeknd-fans-targeted-in-fake-concert-ticket-scams-bitdefender-labs-warns
- Bitdefender, 'Scamscriptions': How to Recognize and Avoid Deceptive Subscriptions (2025), available at: https://www.bitdefender.com/en-us/blog/hotforsecurity/scamscriptions-how-to-recognize-and-avoid-deceptive-subscriptions

- Bitdefender, How to Spot and Avoid Sponsorship Scams (2024), available at: https://www.bitdefender.co.uk/consumer/support/answer/107805/
- BlueVoyant, The rising Threat of Search Engine Ad Abuse (2024), available at: https://www.bluevoyant.com/blog/the-rising-threat-of-search-engine-ad-abuse.
- C2PA, C2PA Content Credentials Explained: Addressing Common Questions and Updates (2025), available at: https://c2pa.org/wp-content/uploads/sites/33/2025/10/content_credentials_wp_0925.pdf.
- CERT Polska, Ad fraud on large online platforms (2024), available at: https://cert.pl/en/posts/2024/12/Ad-fraud-on-large-online-platforms/
- Chainalysis, Record $17 Billion Estimated Stolen in Crypto Scams and Fraud in 2025 as Impersonation Tactics and AI Enablement Surge (2026), available at: https://www.chainalysis.com/blog/crypto-scams-2026/
- Check Point, Inside Europe's AI-Fuelled GLP-1 Scam Epidemic (2025), available at: https://blog.checkpoint.com/research/inside-europes-ai-fuelled-glp-1-scam-epidemic-how-criminal-networks-are-hijacking-the-identities-of-the-nhs-aemps-ansm-bfarm-and-aifa-to-sell-fake-weight-loss-products/
- Content Authenticity Initiative / C2PA, The Content Authenticity Initiative: Setting the Standard for Digital Content Attribution (2020), available at: https://acrobat.adobe.com/link/track?uri=urn%3Aaaid%3Ascds%3AUS%3A2c6361d5-b8da-4aca-89bd-1ed66cd22d19.
- Crowdstrike, What is SEO poisoning? (2023), available at: https://www.crowdstrike.com/en-us/cybersecurity-101/social-engineering/seo-poisoning/.
- Didit, Fraud Syndicates: How Organized Criminals Bypass KYC (2026), available at: https://didit.me/blog/fraud-syndicates-bypass-kyc/
- Dock Labs, KYC fraud: 7 strategies to prevent KYC fraud (2026), available at: https://www.dock.io/post/kyc-fraud#what-is-kyc-fraud
- European Advertising Standards Alliance (EASA), EASA Best Practice Recommendation on Influencer Marketing Guidance 2023 (2023), available at: https://www.easa-alliance.org/publications/best-practice-recommendation-on-influencer-marketing-guidance_v2023/
- European Advertising Standards Alliance (EASA), Responsible influencer marketing, available at: https://www.easa-alliance.org/responsible-influence/
- FBF, Perceptions et comportements des français en matière de cybersécurité – Étude Harris Interactive 2024 (2024), available at: https://www.fbf.fr/fr/etude-2024-sur-les-perceptions-et-comportements-des-francais-en-matiere-de-cybersecurite/
- Fraud.com, NFT Scams – Real-life story, available at: https://www.fraud.com/post/nft-scams-a-real-life-story.
- Gen, The Scam Ad Machine (2026), available at: https://www.gendigital.com/blog/insights/research/scam-ad-machine-meta
- Gen, The Scam Ad Machine: Part II (2026), available at: https://www.gendigital.com/blog/insights/research/the-scam-ad-machine-part-ll
- Gen, Gen Q3/2025 Threat Report (2025), available at: https://www.gendigital.com/blog/insights/reports/threat-report-q3-2025
- Gen, Gen Q4/2024 Threat Report (2024), available at: https://www.gendigital.com/blog/insights/reports/threat-report-q4-2024

- Global Anti-Scam Alliance, Global State of Scams – 2025 (2025), available at: https://gasa.org/knowledge-base/reports/global-state-of-scams-2025
- Global Anti-Scam Alliance, State of Scams in Belgium – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_f4d15a699656439fb4ebfb9a5bdd55a1.pdf
- Global Anti-Scam Alliance, State of Scams in Denmark – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_3333c506a2274110988e0092bb9b04d4.pdf
- Global Anti-Scam Alliance, State of Scams in France – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_fa620227910a4e8ebc06c0cd5e036614.pdf
- Global Anti-Scam Alliance, State of Scams in Germany – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/73a75e_dbef245762ef487797354a803b67eb14.pdf
- Global Anti-Scam Alliance, State of Scams in Italy – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_90a4ada9f8be41b3b601995d679f5d30.pdf
- Global Anti-Scam Alliance, State of Scams in Spain – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_737deba33aa546088296efc5ab7dff26.pdf
- Global Anti-Scam Alliance, State of Scams in the Netherlands – 2025 Report (2025), available at: https://226ef3c9-b82f-4556-974f-4820030abfb0.filesusr.com/ugd/2594f1_e4b2335bcebd496cab156f9a2440b6e1.pdf
- Graphika, Cutting Through the Noise: Social Media Scam Tactics Targeting Financial Institutions in 2025 (2025), available at: https://graphika.com/posts/cutting-through-the-noise-social-media-scam-tactics-targeting-financial-institutions-in-2025
- Group IB, Pig Butchering Alert: Fraudulent Trading App targeted iOS and Android users (2024), available at: https://www.group-ib.com/blog/pig-butchering/
- Insurance Europe, Insurance Europe response to EC consultation on online fraud (2026), available at: https://www.insuranceeurope.eu/mediaitem/c356079f-c353-4754-a049-1a0054e0b29b/Insurance+Europe+response+to+EC+consultation+on+online+fraud.pdf?inline=1
- Insurance Fraud Bureau, Don't be caught out by fake car insurance – The Result Could Be Crushing, available at: https://www.insurancefraudbureau.org/en/ghost-broking
- ITPro, 'Phishing kits are a force multiplier': Cheap cyber crime kits can be bought on the dark web for less than $25 (2025), available at: https://www.itpro.com/security/cyber-attacks/phishing-kits-cyber-crime-dark-web

- JobScamScore, Job Scam Statistics 2026 (2026), available at: https://jobscamscore.com/guides/job-scam-statistics
- Juniper Research, Fraud-as-a-Service: Inside the Dark Web's Booming Business Model (2024), available at: https://www.juniperresearch.com/resources/blog/fraud-as-a-service-inside-the-dark-webs-booming-business-model/
- Ledger Academy, Airdrop Scams (2025), available at: https://www.ledger.com/academy/glossary/airdrop-scams
- Malwarebytes, Booking.com breach gives scammers what they need to target guests (2026), available at: https://www.malwarebytes.com/blog/data-breaches/2026/04/booking-com-breach-gives-scammers-what-they-need-to-target-guests
- Memyco, Fake Search Ads and Brand Impersonation: Why Takedown Alone Misses the Real Risk (2026), available at: https://www.memcyco.com/fake-search-ads-brand-impersonation.
- Norton, Reservation Hijack Scam: the travel scam that looks exactly like your real hotel booking (2026), available at: https://us.norton.com/blog/online-scams/reservation-hijacking-scam
- Proofpoint, Security Brief: Scammers Create Fraudulent Olympics Ticketing Websites (2024), available at: https://www.proofpoint.com/us/blog/threat-insight/security-brief-scammers-create-fraudulent-olympics-ticketing-websites
- Security Research Labs, BogusBazaar: A criminal network of webshop fraudsters (2024), available at: https://srlabs.de/blog/bogusbazaar
- Solidus Labs, What is a Rug Pull? DeFi Scams Explained (2022), available at: https://www.soliduslabs.com/post/rug-pull-crypto-scams
- StreamCharts, The Hidden Cost of Viewbotting (2025), available at: https://streamscharts.com/reports/viewbotting-whitepaper
- Surfshark, Beware of concert ticket fraud online (2025), available at: https://surfshark.com/research/chart/concert-ticket-fraud
- Sumsub, Identity Fraud Report 2024 (2024), available at: https://sumsub.com/fraud-report-2024/.
- Take Five, Ticket scams, available at: https://www.takefive-stopfraud.org.uk/protect-yourself/ticket-scams/
- Tech Transparency Project, Meta Awash in Deepfake Scam Ads (2025), available at: https://www.techtransparencyproject.org/articles/meta-awash-in-deepfake-scam-ads.
- Tenable, Pig Butchering Scam: From Tinder and TikTok to WhatsApp and Telegram, How Scammers Are Stealing Millions in a Long Con (2024), available at: https://www.tenable.com/blog/pig-butchering-scam-tinder-tiktok-whatsapp-telegram-scammers-steal-millions
- Thorn, Trends in Financal Sextortion – An investigation of sextortion reports in NCMEC CyberTipline data (2024), available at: https://info.thorn.org/hubfs/Research/Thorn_TrendsInFinancialSextortion_June2024.pdf
- VectraAI, SEO Poisoning Attacks: How Cybercriminals Weaponize Search Results (2025), available at: https://www.vectra.ai/topics/seo-poisoning

Risk Assessment Reports by VLOPs and VLOSEs

- AliExpress, Digital Services Act Annual Risk Assessment Report (2025), available at: https://files.alicdn.com/tpsservice/b1e5c47188c3d161d91de46033988a69.pdf
- Amazon Store, Risk Assessment 2025 (2025), available at: https://trustworthyshopping.aboutamazon.com/eu-dsa-risk-assessment-report-amazon-2025
- Apple AppStore, App Store – Third Report on Risk Assessment and Risk Mitigation Measures (2025), available at: https://www.apple.com/legal/dsa/20251119_app-store_risk-assessment-report_non-confidential.pdf
- Aylo, Report on the results of the risk assessment for Pornhub.com pursuant to Article 34 of the Digital Services Act (2025), available at: https://ei.phncdn.com/static/misc/legal/Risk_Assessment_for_Pornhub_April_2025_1752958273.pdf
- Bing, Bing Systemic Risk Assessment Report (2025), available at: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/bade/documents/products-and-services/en-us/digitalsafety/August-2025-Microsoft-Bing-Systemic-Risk-Assessment-Report-EU-Digital-Services-Act.pdf
- Booking.com, Digital Services Act, 2025 – Report on the results of the Systemic Risk Assessment and Mitigation Measures conducted by Booking.com B.V. under the Digital Services Act (2025), available at: https://q-xx.bstatic.com/data/mobile/2025%20-%20Systemic%20risk%20assessment%20and%20mitigation%20measures%20completion%20report.pdf
- Facebook (Meta), Regulation (EU) 2022/2065 Digital Services Act (DSA) Systemic Risk Assessment and Mitigation Report for Facebook (2025), available at: https://scontent.fflr4-1.fna.fbcdn.net/
- Google, Report of Systemic Risk Assessments (2025), available at: https://storage.googleapis.com/transparencyreport/report-downloads/dsa-risk-assessment_2025-8-28_2025-8-28_en_v1.pdf
- Instagram (Meta), Regulation (EU) 2022/2065 Digital Services Act (DSA) Systemic Risk Assessment and Mitigation Report for Instagram (2025), available at: https://scontent.fflr4-1.fna.fbcdn.net/
- LinkedIn, Systemic Risk Assessment (2025), available at: https://content.linkedin.com/content/dam/help/tns/legal/01-LinkedIn-DSA-2025-SRA-Report-August-2025.pdf
- Pinterest, Digital Services Act Risk Assessment and Mitigation Report (2025), available at: https://help.pinterest.com/sites/default/files/dsa/Pinterest-2025-DSA-Systemic-Risk-Assessment-and-Mitigation-Report.pdf
- Shein, Risk Assessment 2025 Report (2025), available at: https://drive.google.com/file/d/1op8QTl7GL4MpIB131Tx9QU2-HEHK_X_v/view
- Snapchat, Snap DSA Report. Risk Assessment Results and Mitigations (2025), available at: https://downloads.ctfassets.net/kw9k15zxztrs/2AsrmglaVlYdydFRiWGLnj/0e82a

c4bf9e1ba24068f141d97c00581/Redacted_2025_DSA_Risk_Assessment_Redacted.pdf

- Temu, Risk Assessment and Mitigation Report (2025), available at: https://www.dropbox.com/scl/fi/o15r3rzd6emrc0rxcarhr/DSA-Risk-Assessment-and-Mitigation-Report-2025.pdf
- TikTok, DSA Risk Assessment 2025 Report (2025), available at: https://sf16-va.tiktokcdn.com/obj/eden-va2/zayvwlY_fjulyhwzuhy/ljhwZthlaukjlkulzlp/DSA/DSARiskAssessmentReport-TikTokTechnologyLimited-2025.pdf
- Wikipedia, Wikipedia EU DSA Systemic Risk Assessment (2025), available at: https://foundation.wikimedia.org/wiki/File:WMF_24-25_Wikipedia_EU_DSA_Systemic_Risk_Assessment.zip
- X, Report Setting Out the Results of X Internet Unlimited Company Risk Assessment Pursuant to Article 34 EU Digital Services Act (2025), available at: https://transparency.x.com/content/dam/transparency-twitter/dsa/2025-x-dsa-sra-summary-report.pdf
- XNXX, Risk Assessment Report on the results of the Systemic Risk Assessment Under the Regulation (EU) 2022/2065 Digital Services Act (DSA) conducted for XNXX.COM (2025), available at: https://www.dropbox.com/scl/fi/cc4peepdm7cax1x79hwu6/XNXX-Risk-Assessment-Report-2025.pdf
- XVideos, Risk Assessment Report on the results of the Systemic Risk Assessment Under the Regulation (EU) 2022/2065 Digital Services Act (DSA) (2025), available at: https://www.dropbox.com/scl/fi/8vw0dyixxifxzle0bfbbz/2025-WGCZ_XVIDEOS_Risk-Assessment-Report_23_April_2025.pdf
- Zalando, Risk Report Digital Services Act 2025 (2025), available at: https://drive.google.com/file/d/1OmJbfMU21uKRx8tLJ6E1EzivJJr_oPzl/view

Independent Audit Reports

- BDO, X's Digital Services Act (DSA) Report, available at: https://www.dropbox.com/scl/fi/7u4piajjcsdczwk9v0r3p/2025-x-dsa-audit-report.pdf.
- Certicom, Independent Audit Report on XNXX.com, available at: https://www.dropbox.com/scl/fi/uoahy5diltdjsn7x4ayrh/XNXX-Independent-Audit-Report-2025.pdf.
- Certicom, Independent Audit Report on XVideos.com, available at: https://www.dropbox.com/scl/fi/jmajkhxld16ehp044adtb/2025-Audit-Report.pdf.
- Deloitte, Booking.com B.V. Digital Services Act (DSA) Assurance Report, available at: https://www.dropbox.com/scl/fi/pct8bi29kykqq1tda58ct/2025-Audit-report.pdf.
- Deloitte, Independent Practitioner's Assurance Report on Zalando SE's compliance with the Digital Services Act, available at: https://www.dropbox.com/scl/fi/n8dnm429o1r17uwbc7lbv/2025-Audit-Report.pdf.
- Deloitte, LinkedIn's Digital Services Act (DSA) and Code of Conduct on Countering Illegal Hate Speech Online (Code of Conduct) Report, available at: https://www.dropbox.com/scl/fi/nget5qj8vi7d3k778ybus/2025-Audit-Report.pdf.

- Deloitte, Microsoft Bing's Digital Services Act (DSA) Report, available at: https://www.dropbox.com/scl/fi/p7t7crqw6w54yu4qp98g2/August-2025-Microsoft-Bing-Audit-Report-EU-Digital-Services-Act.pdf.
- Deloitte, SHEIN – DSA Assurance Report, available at: https://www.dropbox.com/scl/fi/vaxfl4vttxcg8wj78feb4/2025-Audit-Report.pdf.
- EY, Independent Audit on Facebook, available at: https://www.dropbox.com/scl/fi/fbx16f0ieakgkersk2ctv/2025-Audit-Report.pdf.
- EY, Independent Audit on Google Maps – Digital Services Act, available at: https://www.dropbox.com/scl/fi/iuyiw6po4ws12ikpaxy4f/2025-Audit-Report.pdf.
- EY, Independent Audit on Google Play – Digital Services Act, available at: https://www.dropbox.com/scl/fi/81133n2f15wdsbmu8gx7n/2025-Audit-report.pdf.
- EY, Independent Audit on Google Search – Digital Services Act, available at: https://www.dropbox.com/scl/fi/o6z386lexmp3leeqtj0v4/2025-Audit-report.pdf.
- EY, Independent Audit on Google Shopping – Digital Services Act, available at: https://www.dropbox.com/scl/fi/ti6dfeps05kwr5207h69m/2025-Audit-report.pdf.
- EY, Independent Audit on Instagram, available at: https://www.dropbox.com/scl/fi/v3n2nxj7mg0m0gr71ljac/2025-Audit-Report.pdf.
- EY, Independent Audit on Pinterest, available at: https://www.dropbox.com/scl/fi/kr9mkl9949jwkk53hcop0/Independent-Audit-of-Pinterest-DSA-Redacted-11102025.pdf.
- EY, Independent Audit on Snapchat, available at: https://www.dropbox.com/scl/fi/i93vef6fc38fhc2kgtakf/DSA_and_Hate_Speech_Code_of_Conduct_Reporting_Package_-_Snapchat_2025_Redacted.pdf.
- EY, Independent Audit on TEMU, available at: https://www.dropbox.com/scl/fi/buv4tarf7mkf11vq5ec5n/DSA-Audit-Report-2025.pdf.
- EY, Independent Audit on the App Store, available at: https://www.dropbox.com/scl/fi/htdwuqum9fljh7mw7fjkn/20251119_app-store_reasonable-assurance-report_non-confidential.pdf.
- FTI Consulting, Independent Audit – Article 37 of Regulation (EU) 2022/2065 (Digital Services Act) [Pornhub], available at: https://www.dropbox.com/scl/fi/s1wvtx9ixpzcwemp7fsbs/Audit_Report_for_Pornhub_April_2025_1753199885.pdf.
- FTI Consulting, Independent Audit of AliExpress – Article 37 of Regulation (EU) 2022/2065 (Digital Services Act), available at: https://www.dropbox.com/scl/fi/8mn8wigchllrxpp4kypkz/2025-Audit-Report.pdf.
- Holistic AI, Independent Audit on Wikipedia, available at: https://www.dropbox.com/scl/fo/mygrijkpirx0h48mrzwsf/AFDUlK8fCKnIV9a6CB0KkrM.
- KPMG, DSA Assurance Report – Independent practitioner's assurance report concerning Regulation (EU) 2022/2065, the Digital Services Act (DSA) [Amazon], available at: https://www.dropbox.com/scl/fi/4weflzsc8jqs2zhr0xyq1/eu-dsa-audit-report-amazon-2025.pdf.
- KPMG, DSA Assurance Report – Independent practitioner's assurance report concerning Regulation (EU) 2022/2065, the Digital Services Act (DSA) [TikTok Technology Limited], available at: https://www.dropbox.com/scl/fi/nldbvg99c59xrfmvja8qm/DSAAssuranceReport-TikTokTechnologyLimited-2025.pdf.

Public Policies and Information from VLOPs/VLOSEs

- Google Ads and Commerce Blog, Introducing a new era of AI-powered ads with Google (2023), available at: https://blog.google/products/ads-commerce/ai-powered-ads-google-marketing-live/
- Google Search Central, Spam policies for Google web search, available at: https://developers.google.com/search/docs/essentials/spam-policies
- Google, Apply for Election Ads verification, available at: https://support.google.com/adspolicy/troubleshooter/9973345?hl=en
- Google, Fighting Search Scams with AI (2024), available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Search-Scam-Report-0508.pdf
- Google, Financial Services Verification, available at: https://support.google.com/adspolicy/answer/12390454?hl=en
- Google, Fraud and Scams Advisory (2025), available at: https://blog.google/innovation-and-ai/technology/safety-security/fraud-and-scams-advisory-november-2025/
- Google, How We Kept Google Play and the Android App Ecosystem Safe in 2024 (2025), available at: https://blog.google/security/how-we-kept-google-play-android-app-ecosystem-safe-2024/
- Google, Tackling scams and fraud together – Google white paper (2024), available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Tackling_scams_and_fraud_together.pdf
- LinkedIn Engineering, Automated Fake Account Detection at LinkedIn (2022), available at: https://www.linkedin.com/blog/engineering/trust-and-safety/automated-fake-account-detection-at-linkedin
- Meta, Advertising Standards, available at: https://transparency.meta.com/policies/ad-standards/.
- Meta, Avoiding Investment and Payment Scams Online (2025), available at: https://about.fb.com/news/2025/05/avoiding-investment-payment-scams-online/
- Meta, Confirm your identity to run ads about social issues, elections or politics, available at: https://www.facebook.com/business/help/2992964394067299?id=288762101909005
- Meta, Cracking Down on Organised Crime Scam Centres (2024), available at: https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/
- Meta, Fighting scammers: Protecting people with new technology and partnerships (2026), available at: https://about.fb.com/news/2026/03/fighting-scammers-protecting-people-with-new-technology-and-partnerships/
- Meta, Meta launches new anti-scam tools, deploys AI technology to fight scammers and protect people (2026), available at: https://about.fb.com/news/2026/03/meta-launches-new-anti-scam-tools-deploys-ai-technology-to-fight-scammers-and-protect-people/
- Meta, Protect your Brand with Meta Verified, available at: https://www.meta.com/en-gb/meta-verified/

- Meta, Scams Are Bad for Business: Our Ongoing Efforts to Fight Fraud (2025), available at: https://about.fb.com/news/2025/12/scams-are-bad-for-business-metas-efforts-to-fight-fraud/
- Meta, Sharing new open source protection tools and advancements in AI privacy and security (2025), available at: https://ai.meta.com/blog/ai-defenders-program-llama-protection-tools/
- Microsoft, New steps to combat disinformation and deepfakes with NewsGuard's Video Authenticator (2020), available at: https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator
- TikTok Business Resource Center, Advertiser Account Policy (2025), available at: https://ads.tiktok.com/resources/help/article/actor-policy
- TikTok, Deceptive Practices (2025), available at: https://ads.tiktok.com/help/article/tiktok-ads-policy-deceptive-practices
- X, Ads Policies: Deceptive & Fraudulent Content, available at: https://business.x.com/en/help/ads-policies
- YouTube Help, Disclosing use of GenAI content, available at: https://support.google.com/youtube/answer/14328491

Annex II – Interview guide for Task 1

Please introduce yourself and briefly explain your expertise and your experience with online financial scams.

General overview of online financial scams

1. What are the main types of financial scams encountered on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs), as designated under Regulation (EU) 2022/2065?

2. Which are the most frequent types of financial scams per different types of online platforms?

3. Who are the primary actors involved in operating financial scams?

Risk factors on designated services

4. What particular risk factors, associated with the architecture and functionalities of designated services, are leveraged to disseminate online financial scams?

5. Which dissemination methods generate the highest levels of user engagement or exposure?

Cross-cutting operational or behavioural models

6. What methods or tools do offenders use to carry out financial scams?

7. How are technological developments affecting the scale and sophistication of financial scams?
8. What trends are emerging in the evolution of online financial scams?

Impact on users

9. Who are the victims of financial scams, and which user groups are particularly vulnerable?

10. What types of harm do financial scams cause to users?

11. What is the social impact of financial scams on individual users and on the wider public?

12. What is the economic impact of financial scams on individual users and on the wider digital economy?

Countermeasures

13. Are there any technologies, processes, or approaches against online financial scams that you consider promising for the near future?

14. Have you observed any emerging or innovative strategies that address the risk factors associated with the designated services?

Closing questions

15. What other aspects of online financial scams that we have not discussed would you like to mention?

16. Is there any relevant literature on this topic that you would like to share?

Annex III – Interview guide for Task 2

Please introduce yourself and briefly mention your expertise and experience with online financial scams.

General overview

1) What does the current landscape of countermeasures against online financial scams look like?

2) Are there specific technologies, processes, or approaches that you consider promising for the near future?

Countermeasures at service level

3) Which are the most common methods used to verify the identity of online actors before they reach the public (e.g., in advertising or account creation)?

4) Which are the primary methods currently used to detect scam activity online?

5) Beyond content removal, which methods are used to disrupt the scammers' operations?

6) When a scam is active, are there any types of "friction" or disruptive measures that are being deployed to protect the end-user?

7) What role do user-facing tools (e.g., reporting systems, browser warnings, or in-app alerts) play in the broader counterstrategy?

8) How do VLOPs and VLOSEs cooperate with third parties (e.g., national authorities, civil society) in countering online financial scams?

Countermeasures at operational level

9) Which specific technologies are currently playing the largest role in detecting and neutralising financial scams?

10) What measures are being taken to target the infrastructure behind online financial scams?

Limitations and adaptations

11) What are the most significant limitations in the current system of countermeasures that scammers continue to exploit?

12) How do scammers typically react to the introduction of new countermeasures, and what methods do they use to bypass or undermine these controls?

Closing questions

13) What other aspects of countering online financial scams that we have not discussed would you like to mention?

14) Is there specific research on the topic of today’s interview that you would like to share?

Annex IV - Workshop Report

The Digital Services Act (DSA) introduces a comprehensive set of harmonised rules for providers of intermediary services. The DSA introduces due diligence obligations for all intermediary services, with additional, more stringent requirements for designated Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). These include obligations related to transparency, notice-and-action mechanisms, advertising, and recommender systems, as well as specific rules to address systemic risks that may arise from the functioning and use of their services.

Amongst those systemic risks, online financial scams stand out as deceptive practices carried out through online platforms that aim to mislead users into disclosing financial data or transferring funds. These practices encompass a wide range of illegal or harmful behaviours, including, *inter alia,* fraudulent investment schemes, e-commerce scams or romance scams. Online financial scams are characterised by diverse operational models and increasingly sophisticated tactics, often leveraging platform functionalities and technological developments to maximise reach and effectiveness.

In this context, the European Commission (DG CONNECT – Directorate General for Communications Networks, Content and Technology) has commissioned a **Support contract on financial scams Study**, which is being carried out by Spark Legal and Policy Consulting, in collaboration with Open Evidence.

The study aimed to develop a comprehensive understanding of how online financial scams manifest across different types of VLOPs and VLOSEs, how they are operationalised, and what harms they generate. A key component of the study was the development of a typological mapping of financial scam formats and of an overview of the existing and emerging countermeasures against them. This mapping examined how scams operate in practice, including their underlying operational logic, the role of platform design and functionalities in facilitating or incentivising scam activities, and the countermeasures adopted by service providers.

The engagement of stakeholders and independent experts was central to ensuring the robustness and relevance of the study's findings. The multi-stakeholder workshop on online financial scams brought together representatives from civil society, industry and academia, as well as from European institutions and national authorities, to discuss the study's findings.

The workshop was organised on 22 June 2026 (08:45-13:45) in a hybrid format at the European Commission – Centre de Conférence Albert Borschette in Brussels and online. In total, there were 73 participants, excluding the study team and the project officers from DG CONNECT. The table below presents the categories of organisations represented and the number of participants for each.

Table 13 - Overview of workshop participants

Type of organisation	Number of participants
EU institutions and agencies	12
National authorities	34
Civil society and consumer protection organisations	12
Trusted flaggers	6

Type of organisation	Number of participants
Industry	9

The workshop provided an opportunity to present and validate the identified scam typologies, to discuss the role of platform features in enabling or mitigating scams, and to exchange views on the existing and potential countermeasures against online scams. It supported the study team in refining its findings and contributed to developing evidence-based, policy-relevant recommendations under the DSA framework. The workshop agenda is presented below.

Table 14 - Workshop agenda

Time	Agenda item
08:45-09:00	Introductory coffee
09:00-09:15	Introduction
09:15-09:40	Typological mapping of online scams
09:40-10:00	Guided discussion
10:00-10:20	Risk factors
10:20-10:45	Guided discussion
10:45-11:00	Coffee break
11:00-11:25	Countermeasures against online financial scams
11:25-11:45	Guided discussion
11:45-12:10	Case studies
12:10-12:30	Guided discussion
12:30-12:45	Closing remarks
12:45-13:45	Lunch

During the event, participants were invited to share their views under the Chatham House Rule. To allow for elaboration, participants were also invited to provide written feedback and input within 5 working days of the event (30 June 2026). The same non-attribution rules applied to written contributions, which were submitted via email and had an unstructured format. Written contributions were submitted only by organisations that attended the workshop.

The following sections summarise the input provided by the participants in response to the presentation of the study team's preliminary findings and the discussion questions posed by it. Participants' views are reported below without attribution. Some of the participants' claims could not be cross-checked and verified, as they refer to their own experience. The relevant references are included where participants referred to publicly available data. **Any views or opinions expressed below belong to participants in the workshop and do not represent the official opinion of the European Commission**.

1. Scam Typology

The study team presented its preliminary typology of online financial scams, briefly describing each category of scams and the types of fraudulent behaviours it includes. Following the presentation, the audience was invited to provide their input as part of a structured discussion session, following the discussion questions below.

Discussion Question

1. The study maps a wide and growing landscape of online financial scams. Do you recognise these types of scams from your own experience? Are there scam types or trends that you think are missing or underrepresented? Explain why.

Overall, the participants in the workshop expressed agreement with the preliminary typology proposed by the study team. As a methodological note, a participant recommended distinguishing between online scams with financial consequences (primary objective: to extract money) and financial scams *per se*, as the latter are understood as scams that impersonate banks or payment providers.

Additional data on prevalence was shared by the participants, with reference made to the recently published EU FRA report on online fraud, the findings of which are based on interviews with 26,000 individuals concerning their experiences with online fraud.[1397] That report finds that the most prevalent type of online scam was fake online shopping (35% of victims), followed by impersonation scams (25%), especially impersonation of family members.[1398] The findings of that report were confirmed by multiple participants.

In addition to the impersonation of family members, it was highlighted that impersonation scams also extend to the impersonation of public authorities offering government aid or police contacting victims about a crime. Another participant also highlighted that impersonation can be used to carry out other scams, referring to the use of the likeness of national authorities (e.g. the President of Romania) and wealthy business figures to promote investment scams.

Another participant also highlighted the role that account hijacking plays in rental scams, noting that scammers take over real accounts and use them for fraud, thus benefiting from the credibility afforded by the consumers' trust in the accommodation platform concerned.

One participant noted that multiple types of scams or behaviours identified by the study team operate in a grey area, referring to *'finfluencers'* promoting investment scams or the use of exaggerated and miraculous claims as part of health scams.

Some recommendations for refining the scope of the typological mapping were made by participants, as follows:

- One participant recommended that phishing emails be added to the scope – not only those designed to steal data, but also those that lure victims into approving payments. On this point, another participant suggested the inclusion of phishing under a category of impersonation scams, referring to malicious actors posing as other entities to trick victims into sharing information.

[1397] EU FRA, Online fraud - people's experiences across the EU (2026), available at: https://fra.europa.eu/en/publication/2026/victims-online-fraud.

[1398] ibid.

- Another participant expressed that, in their opinion, gaming apps that appear free to play but become unplayable without payment should also be considered as a type of scam operating in a grey area. Virtual currencies are hidden as coins or items, and fake scarcity is involved. Fake accounts create the illusion of interacting with other players. They expressed that these apps primarily target minors and represent a grey zone involving coordinated operations to extract money.
- Another member of the audience suggested including digital services scams (non-delivery or subscription) and payment scams (fake banking sites used in phishing and leading to identity theft) as distinct sub-categories.
- It was also proposed to rename 'romance scams' as 'sentimental scams' in recognition of the fact that scammers exploit not only romantic connections but also family bonds – for example, messages claiming "Mom, I got robbed, this is a new phone I just bought."
- Tech support scams were also proposed for inclusion in the typology. This phenomenon refers to scammers convincing victims of non-existent issues or intercepting legitimate support requests, often leading them to download malicious software.
- Lastly, business email compromise (BEC) and CEO fraud were recommended for inclusion under the employment and collaboration scams category.

Discussion Question

2. Scammers are known to quickly adapt their operations to onboard new technologies and avoid detection. What new scam types or behaviours have emerged in recent years because of this adaptation process? Please explain the role that new technologies play in this regard.

Participants identified several new scam types and behaviours that have emerged as a result of scammers adapting their operations to onboard new technologies. It was also emphasised that GenAI has become a major component in investment scams and that this should be a focus area. The risk of GenAI-related scams targeting children was also raised, including a growing trend of sextortion since 2023, nudification of benign images of children, and the creation of AI-generated scripts used to conduct scams.

One participant discussed findings from a study on online advertising, highlighting malvertising – advertising that promotes or delivers malware to users' devices – with impacts ranging from ransomware attacks to the creation of networks of bots for denial-of-service attacks.[1399] The concept of "internet trapping" was introduced.

Another participant noted the importance of timing in scam campaigns, citing examples such as romance scams around Valentine's Day, fake jerseys during the World Cup, and Christmas-themed campaigns. Another participant recommended treating AI as a cross-category tool, important for effective enforcement, and observed that many scams are not in written form but occur in video format or via phone calls.

Written contributions highlighted prompt injection and jailbreaking of AI systems as a significant emerging concern. Beyond the misuse of AI for bot automation, profiling, or deepfake abuse, threat actors may also exploit legitimate AI-driven services through techniques such as penetration testing of AI agents, assistants, chatbots, and machine

[1399] European Commission, Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers (2023), available at: https://op.europa.eu/en/publication-detail/-/publication/8b950a43-a141-11ed-b508-01aa75ed71a1/.

learning models, representing a growing threat to services deployed by legitimate entities.

AI companions and SEO poisoning of large language models were also identified by participants as emerging threats, with AI agents subject to prompt injection directing users to scam websites. It was emphasised that scams exist wherever humans interact and that scammers will always attempt to outsmart the system.

Discussion Question

3. Several scam categories in the report, for example artificial streaming scams, insurance scams or subscription scams, receive comparatively less public attention than investment or fake webshop scams. Is this difference in media coverage proportional to their prevalence? Do you consider these categories of scams to be adequately understood and documented? If not, please explain why.

Participants confirmed that subscription scams remain very present. Written contributions also identified several reasons for the lower visibility of certain scam categories. For example, it was mentioned that victims of social or psychological manipulation often feel shame, making them less likely to report, which in turn limits the evidence available to media. Additionally, some novel scam types target specific population segments or professional profiles, resulting in lower volumes compared to broader scam categories. Furthermore, certain scam types – such as insurance scams – affect complex processes that may take more time to execute, making them harder to exploit at scale and thus less visible.

2. Risk Factors

The study team presented its analysis of the risk factors associated with the design and functioning of designated services that contribute to the dissemination and impact of online financial scams. Following the presentation, participants were invited to provide their input as part of a structured discussion session, following the discussion questions below.

Discussion Question

4. The report identifies online advertising as one of the dominant dissemination channels for most scam types. Does this reflect what you are observing on the ground? How do scammers exploit ad placements?

Several participants confirmed that online advertising serves as a primary dissemination channel for scam operations. One participant stated that platforms have little incentive to combat scam advertising because they generate revenue from ads. Another participant emphasised that scam advertising is fundamentally a numbers game, referring to a Reuters report that alleges Meta would derive a significant percentage of its revenue from scam ads.[1400] This claim could not be independently verified by the study team.

A written contribution recommended further exploration of the actual financial advantage that VLOPs and VLOSEs gain from third-party advertisement volumes, suggesting that greater transparency requirements or the development of metrics could provide better

[1400] Reuters, Meta is earning a fortune on a deluge of fraudulent ads, documents show (2025), available at: https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

insight into whether platforms have secondary interests in not being as severe as possible against malvertising.

A participant noted what they believe to be a regulatory gap in the DSA: scam advertising occurs on the open web via intermediaries outside the scope of the instrument, and many publishers reportedly feel pressured to run low-quality ads to meet revenue goals. This claim could not be independently verified by the study team.

One participant also referenced established standards for the content of advertising and ongoing programmes supporting the dissemination of good practices among content creators, drawing from the Ethical Standards for Content Creators (https://adethics.org/i-work-with-content-creators/) initiative.

One participant representing a trusted flagger reported taking down 70,000 Facebook pages carrying 8.2 million ads shown to 3.3 billion contacts in the EU over five months and noted that technologies such as link cloaking are becoming prevalent, complicating criminal investigations. This claim could not be independently verified by the study team.

The evolving nature of scam mediums was also highlighted. New trends involve augmented and virtual reality scams (including through VR glasses), making scams harder to recognise as they no longer resemble traditional advertisements. Streaming was identified as increasingly exploited for scamming purposes, with platforms allegedly lacking the capacity to monitor all streaming content. Asking for "gifts" on streaming platforms was identified as a potential form of scam.

Discussion Question

5. What features of the VLOPs and VLOSEs' advertising systems enable scammers' use of ads for the dissemination of fraudulent content? Please provide evidence to support your argument.

Participants offered several perspectives on how advertising systems enable scammers. One participant observed that the risk factors identified in the workshop resemble dissemination channels rather than risk factors per se, noting that advertising systems are not a risk factor as such, but the way they are used is problematic. On the contrary, another participant challenged the use of the term "exploit," observing that it implies the scammer is deliberately deceiving the service providers, whereas there are situations where scam behaviours are facilitated through a lack of diligence in adapting and shaping countermeasures – to exemplify, the participant referred to a report that finds that some platforms would allow advertisers to register only with a string of numbers.[1401] In the opinion of this participant, the lack of consistent prevention and detection mechanisms on online platforms is conducive to scam behaviour, without the need for scammers to take additional steps to circumvent (and thus exploit) the functioning of their services.

From the perspective of advertising standards, enforcement is reportedly challenging, with participants noting that standards only work when platforms are dedicated to

[1401] AI Forensics, Meta Ads: A Pill Hard to Swallow (2024), available at: https://aiforensics.org/uploads/meta_health.pdf

upholding codes. The International Chamber of Commerce (ICC) was noted to have a code on advertising and to collaborate with GASA.[1402]

A participant reported that public investigations claim that at least 30% of ads published on Meta's platforms were scams, and that the ad library needs improvement.[1403]

Discussion Question

6. The report notes that recommender systems prioritise highly engaging content, and that content amplification applies equally to legitimate and fraudulent content, and scam material exploits this neutrality. In your experience, what role do recommender systems play in the dissemination of online financial scams? Please provide evidence to support your argument.

One participant noted that platforms have a role not only in the dissemination and amplification of scam content but also in indirectly shaping which scam formats will be more successful than others. Recommender systems contribute to this dynamic, as scammers test visibility and success rates of their content on platforms.

Discussion Question

7. The report describes a recurring cross-platform pathway in which victims are first contacted through paid ads or organic social media content, then redirected to fraudulent websites or payment services. Some configurations include private messaging applications as an intermediary environment. Does this cross-platform chain adequately reflect the scam journeys you have observed? Are there stages or intermediary environments that deserve greater emphasis?

Participants highlighted the cross-platform nature of scam operations. One participant observed that scammers exploit digital advertising to reach consumers, but that rigid one-size-fits-all verification thresholds do not help, recommending a more flexible, risk-based approach.

Cross-sector collaboration (involving social media, banks, private messaging, civil society) was described as necessary because victims are moved across platforms. It was noted that criminals commonly jump between platforms, making traceability difficult. Participants suggested that AI can be leveraged as a countermeasure to identify scam patterns, and that end-to-end encryption does not preclude enforcement – machine learning can identify patterns.

Another participant stated that payment is essential for fraud, noting existing efforts across multiple industry sectors, including the financial services one, to tackle fraud and cooperate with other stakeholders through multi-stakeholder groups and hosted workshops.

Discussion Question

8. The study identifies a range of risk factors associated with the design and functioning of the designated services. Are there risk factors that you think are

[1402] International Chamber of Commerce, ICC Advertising and Marketing Communications Code (2024), available at: https://iccwbo.org/wp-content/uploads/sites/3/2024/09/ICC_2024_MarketingCode_2024.pdf.

[1403] Gen Digital, The Scam Ad Machine (2026), available at: https://www.gendigital.com/blog/insights/research/scam-ad-machine-meta.

missing or underrepresented? If so, provide evidence to substantiate the role of these risk factors.

One participant noted that the youngest population (aged 15–39) is the most prone to being targeted by scams and recommended that the study highlight how scammers specifically attract this age group and the impact on the types of victims.

3. Countermeasures

The study team presented an overview of the existing countermeasures against online financial scams, covering topics including identity verification, content moderation, reporting mechanisms, user-facing interventions, and cross-platform governance. Following the presentation, participants were invited to provide their input as part of a structured discussion session, following the discussion questions below.

Discussion Question

9. The report identifies high-assurance identity verification methods for placing ads (i.e., requesting identity documents) to be a relevant countermeasure against online scams. What are the added benefits of this measure, and what countervailing considerations should be considered? How can scammers adapt their operations to circumvent this measure?

Participants agreed on the role of identity verification as a countermeasure but raised important caveats. One participant argued that the focus should not be solely on identity verification, since verified accounts can still be fake and fraudulent. Authenticity should be the focus or a parallel focus – linking the ad not just to a real person but to a legitimate economic activity. Friction measures built into platform design were recommended, as many scams rely on urgency and impulsivity. Another participant referenced a paper on online advertising verification, noting advocacy for advertisement verification to be included in EU legislation.[1404] A practical approach to implementation was called for, involving machine learning, access to information, and integration of relevant registers. It was observed that an intermediary – not the financial institution – is often the one that advertises the service, and that IT systems need to be integrated more effectively.

Discussion Question

10. Automated moderation systems are reportedly circumvented through character obfuscation, hidden links, dynamic ads embedding fraudulent content within legitimate campaigns, and link cloaking that serves different content to moderators and users. How does the current content moderation architecture function against online financial scams? What approaches have proven to be effective?

Several participants provided insights on the current state of content moderation. One participant described her experience as a human content reviewer, noting that platforms re-check advertisers only after receiving specific signals (sudden revenue changes, domain changes, change in ownership), with no regular re-checks and no guidance on the effectiveness of measures. Workflows checking for scams reportedly lack quality assurance measures, and user complaints do not trigger escalation or prioritisation. Language moderation was described as dispersed and uneven – scammers use slang

[1404] The Payments Association, The new origin of APP fraud: Evidence of digital platforms' role and the case for shared accountability (2026), available at: https://thepaymentsassociation.org/wp-content/uploads/2026/05/6674_PaymentsAssociation_Whitepaper_AppFraud.pdf.

or game-specific terminology not caught by AI, and human reviewers often lack context. The speed of review was identified as the biggest problem: pressure to review quickly creates false negatives, especially for non-obvious scams. The study team could not independently verify these claims.

Another participant reported that their organisation had submitted reports for ads in 13 countries and that responses from platforms were always the same text translated into different languages, showing no evidence of human intervention. The study team could not independently verify these claims.

On detection, it was observed that while language can be "sneaky," the content of many scam ads is easy to understand (e.g., "get rich today") and does not require sophisticated software to identify. On removal, it was noted that once an ad is assessed as illegal, the associated account should be checked – reference was made to an investigation highlighting cases where clearly fraudulent ads placed by the same advertiser were not removed.[1405] Another participant stated that detection is "not rocket science" and that, in their opinion, the most basic measures are not being employed – pattern recognition and phrase recognition alone would be sufficient to detect many fraudulent ads. Fraudulent ads can also be reactivated under similar names after accounts have been suspended.

A written contribution raised the issue of algorithmic transparency, noting that little to no public transparency is provided about how major services' detection systems work. Within machine learning models, detection methods can significantly vary based on the components that create the neural network and define the classification method, yet very limited information is shared – making actual assessment of these methods borderline impossible. While there are intellectual property and engineering reasons why companies do not fully share model weights or parameters, a transparent description of model components could clarify what biases or filters may be interfering with improved detection.

Discussion Question

11. Scam content may be surfaced to users by recommender systems. What are the current measures implemented by designated services to prevent the amplification of scam content? What are the limitations of these measures? What specific design interventions, beyond content moderation, can meaningfully reduce users' exposure to online scams and fraud?

The participants did not provide any input on this topic. This may indicate a gap in the publicly available data, which may hinder the ability of relevant stakeholders to present an evidence-backed perspective on the matter.

Discussion Question

12. Users, including trusted flaggers, can flag scam content to designated services through reporting mechanisms. What are the limitations and challenges associated with these mechanisms?

Trusted flaggers reported being temporarily blocked when reviewing too many scam sites. From the experience of a contributor, fewer than 1% of the reports filed by their organisation were not taken down. From previous experience, a trusted flagger estimated that 40,000 URLs can be reported in 100 working hours on a relatively submission-friendly system, but equivalent work on platforms that require the reporting

[1405] BEUC, Sponsored by Scammers (2026), available at: https://www.beuc.eu/sites/default/files/publications/BEUC-X-2026-043_Report_Sponsored_by_Scammers.pdf

of content 'one-by-one' (i.e. not offering a bulk reporting option) would require 300,000 hours and is not feasible. The study team could not independently verify these claims.

Standardising reporting tools was described by participants as a straightforward solution that could open doors to submitting more reports. Participants also reported struggling with platforms not providing case IDs.

One participant noted that thanks to the DSA, platforms are now required to share data. However, the amount of data shared on measures taken is, in their opinion, limited – often restricted to automated and non-automated takedowns of ads and accounts. Ad performance data, which platforms possess, would be valuable for understanding the extent of the phenomenon and assessing the effectiveness of countermeasures. A written contribution also highlighted a generalised lack of standardisation in how designated services categorise user reporting, with different labels, procedures, and categorisation approaches – differences that harm intelligence gathering and inhibit the creation of improved datasets for trustworthy detection systems.

Discussion Question

13. Individuals may be over-confident in their ability to detect scams. Fast-scrolling feeds, urgency signals, and countdown timers create environments where critical evaluation is structurally suppressed. What type of user-facing interventions (i.e., friction tools, warnings) could disrupt the state of cognitive overload that scammers exploit? How should these measures be designed to protect vulnerable users without degrading the experience for all users?

One participant raised the introduction of friction in payment functions of platforms. From a risk-based approach, interface features could be structured to impede fraud. Payment features embedded in platforms were identified as an effective channel leveraged by scammers. An "X-by-design" approach was recommended, and it was suggested that payment interfaces merit recognition as a distinct countermeasure category.

Several participants stressed the role of awareness. One stated that awareness and action should not be opposed – awareness-raising is essential alongside preventative action. For example, a participant claimed many advertisers (especially micro-influencers) are not aware of disclosure obligations. A programme to train and certify advertisers was described. Another participant emphasised that research involving interviews with victims showed awareness is the most essential element: victims do not know what to do, where to report, cannot recognise red flags, or feel shame. Significant scope for improvement in victim-support services was identified, and it was noted that timely, real support needs to be provided and that information needs to be more visible.

Discussion Question

14. The report identifies the cross-platform nature of scam operations as a fundamental challenge. No single platform controls the entire scam chain. What governance or collaboration structures can address the fragmented nature of the scam ecosystem? Are there examples of such successful collaborations already implemented?

One participant raised the critical point that there is no effective online enforcement without offline enforcement, including international treaties across jurisdictions. Just-in-time warnings can be employed at friction points (e.g., when encountering an unknown user). Consumer education and awareness were described as important. Collaboration among sectors was highlighted (citing FIRE and GSE initiatives). Hurdles were identified in the form of different and varying interpretations of GDPR measures and ePrivacy rules. Guidance from the European Commission was described as very welcome.

4. Case Studies

The study team presented four case studies examining specific scam typologies in detail. Following the presentation, participants were invited to provide their input as part of a structured discussion session. After being presented with the discussion questions below, participants offered several cross-cutting observations.

- One participant stated that case studies would be more useful if connected to real networks and their impact, rather than being purely theoretical. Specific examples were provided, including pornographic ads that lead to a WhatsApp login that steals the user's account, or illegal gambling services. In relation to investment scams, public statistics were cited indicating 4 billion lost in Europe, while it was reported that illegal (scam) gambling generated almost 81 billion in losses in the EU.[1406]
- Another participant identified as an underlying factor that content is not freely moving on platforms – platforms provide templates for sharing content which may not comply with requirements of EU consumer law. In their opinion, consumer law has not been clearly applied in this area, and cases have been brought against platforms for non-compliance. A further participant stated that no single actor can address the problem alone: the issue goes beyond financial concerns and hinders trust in the Single Market and financial institutions.

Case study A: Finfluencers and Online Coaching on Video-Sharing Platforms

Discussion Question

15. Finfluencers act as a rapidly growing scam vector. Finfluencer content operates in a grey area, raising concerns about compliance with consumer protection legislation. What signals distinguish fraudulent investment schemes from lawful financial content, and how do platforms currently handle that distinction?

A written contribution suggested a threat-actor-based analysis for distinguishing finfluencer behaviour, highlighting that some actors may be genuine but naive influencers who expose less-prepared audiences to potentially damaging financial decisions. Others may be more knowledgeable on financial matters and seeking to exploit caveats to mislead day-to-day investors. Finally, there are outright scammers who maliciously trap victims into projects designed to fail. Differentiating among these types could help identify relevant indicators for detection. Many countries require financial advice to carry disclaimers, and failure to do so can imply liability – more aggressive scams may bypass such concerns to maximise financial returns with minimal time and resource investment.

Discussion Question

16. Finfluencer content that emphasises displays of wealth, creating urgency, and promising exclusivity, is precisely the type of content that performs well under engagement-driven algorithmic logic. Demonetisation of unverified financial advice, mandatory disclaimers, or algorithmic de-amplification of content promoting unrealistic returns are relevant countermeasures that can address this

[1406] Investigate Europe, Scam Europe (2025), available at: https://www.investigate-europe.eu/themes/investigations/-scam-europe; Yield Sec, Illegal Gambling in the EU (2025), available at: https://www.europeancasinoassociation.org/images/News-content/20251120-Yield-Sec/GYS_YS_Illegal_Gambling_in_the_EU_2024_PR_VERSION_11.19.2025.pdf.

risk. In your experience, which of these measures are already implemented by designated services? Have these measures proven to be effective?

The participants did not provide any input on this topic. This may indicate a gap in the publicly available data, which may hinder the ability of relevant stakeholders to present an evidence-backed perspective on the matter.

Case study B: Romance Baiting Scams on Social Media Platforms

Discussion Question

17. Romance baiting represents a deliberate hybridisation of scam models, combining the trust-building dimension of romance scams with the financial extraction mechanics of investment fraud. How do platform detection and moderation systems adapt to hybrid scam typologies that span multiple scam categories, user behaviours, and timeframes?

The participants did not provide any input on this topic. This may indicate a gap in the publicly available data, which may hinder the ability of relevant stakeholders to present an evidence-backed perspective on the matter.

Discussion Question

18. Romance baiting exploits core platform features from the outset, such as profile visibility, follower lists, contact synchronisation, algorithmic recommendation systems, or private messaging functions. Given that these features are designed to foster legitimate social connection, how do platform-level interventions disrupt the romance baiting scam cycle without fundamentally undermining the social functionality of these services?

A written contribution proposed improved detection rules built upon traditional platform parameters. As a practical example, ratio-based metrics within the following/follower model could be used to prevent profiles with anomalous ratios from interacting with profiles displaying normal ratios. This approach could be extended to other indicators, such as the time of creation of profiles and semantic patterns in thematic content interests – for instance, alerting when a profile supposedly representing a teenager primarily interacts with serious adult financial content.

Case study C: Fake Webshop Advertisement on Search Engines

Discussion Question

19. E-commerce scams, including fake webshops, concentrate activity around periods of peak consumer spending. What pre-emptive or real-time measures could search engines implement during known high-risk periods?

A written contribution suggested that requiring VLOPs to officially track and display the evolution of prices within their product pages could be beneficial. This would enable consumers to monitor real prices and market tendencies, while also reducing platforms' room for price obfuscation strategies and unfair advertising.

Discussion Question

20. Ads directing users to fake webshops are deployed by extensive scam networks. What measures do VLOSEs adopt to proactively identify and deprioritise ads exhibiting patterns consistent with fake webshop networks?

The participants did not provide any input on this topic. This may indicate a gap in the publicly available data, which may hinder the ability of relevant stakeholders to present an evidence-backed perspective on the matter.

Case study D: Health and Wellness Scams on E-Commerce Platforms

Discussion Question

21. The structure of product listings on e-commerce platforms, combined with consumer demand for health-related goods, creates an environment that can be manipulated by health and wellness scammers. What design changes (e.g., mandatory seller verification for health product categories, enhanced review authentication, or product claim verification) are implemented by VLOPs to reduce this alignment without impeding legitimate commerce?

The participants did not provide any input on this topic. This may indicate a gap in the publicly available data, which may hinder the ability of relevant stakeholders to present an evidence-backed perspective on the matter.

Discussion Question

22. Health and wellness scams actively rely on misinformation as a propagation vector. Health conspiracies and distrust of mainstream medicine can create a receptive audience for fraudulent alternative treatments, blurring the line between ideological content and commercial fraud. How do e-commerce platforms identify health-related product claims that intersect with known misinformation narratives?

A written contribution drew attention to the creation of echo chambers via major VLOPs, particularly on community-driven platforms where interactions between users can reach high degrees of depth and resonance. Sometimes driven by shame, financial struggles, or lack of knowledge, certain forums and communities can develop into a dangerous environment for the spread of disinformation, fraud, and scams. Increased attention to identifying these echo chambers and their associated themes could represent a first level of defence. An example cited was do-it-yourself methods related to hormone therapy, where users seek support within online groups when unable to find institutionalised care.

Annex V - Overview of measures as reported to have been implemented by designated service providers

The following tables provide information on the countermeasures that VLOPs and VLOSEs claim to have implemented in relation to online financial scams, as reported in their 2025 Risk Assessment reports, 2025 Independent Audit reports and other publicly available platform policies. The table overviews do not assess platform compliance with DSA obligations.

Identity verification measures for account creation

Table 15 - Overview of identity verification measures as reported by the designated services[1407]

Designated service	Measure description
AliExpress	No information is provided by AliExpress on identity verification for the creation of personal accounts, beyond the requirement to confirm the account via SMS or email.
Amazon Store	No information is provided by Amazon Store on identity verification for the creation of personal accounts, beyond the requirement to confirm the account via SMS or email.
Apple AppStore	No information is provided by Apple AppStore on identity verification for the creation of personal accounts, beyond the requirement to confirm the account via SMS or email. Apple AppStore reports that users may provide their payment method and billing information, but this is not a requirement.
Bing	No specific identity verification measures are reported by Bing.
Booking.com	No specific identity verification measures are reported by Booking.com.
Meta designated services	Facebook and Instagram report that they require people to create one account using the name they go by in everyday life that represents their authentic identity. They report that they have processes in place to verify a user's identity on their platforms. Users are asked to provide a copy of an item with their name and date of birth or name and photo on it as proof of identification, such as a photo identification (ID) issued by a government, an ID from a non-government organisation, an official certificate, a licence that includes the user's name, with potential special ID requirements for some cases, such as advertisers running ads about social issues, elections or politics. Facebook

[1407] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

Designated service	Measure description
	and Instagram report that proof of identification is checked for usability and forgery via machine-learning models or human reviewers, then matched against the account profile. Facebook and Instagram report that they may require users to submit their identity documents after account creation if suspicious user activity (scams, phishing) is detected or the user has lost access to their account. Facebook and Instagram also report that they have built classifiers that can help detect if a threat actor that has already been removed from the platform is behind the creation of a new account or other entities and will remove them from their platform(s). It has been reported that they are putting in place new actions to mitigate account takeover by introducing additional verifications, such as log-in challenges, age checks, and verification of contact points.
Google designated services	Google reports that creating a Google Account itself requires only a name, email address, password, and phone number for verification.
LinkedIn	LinkedIn's policies prohibit profiles with false information, including fake identities, misleading or deceptive information regarding business, qualifications, work experience, affiliations, or achievements. LinkedIn reports that members must use a Profile photo that accurately reflects their likeness and not associate with businesses that are not relevant to their professional associations. The platform notes that creating or using another member's account or Profile is not allowed, and sharing LinkedIn accounts is prohibited. LinkedIn reports that it verifies Profiles by performing a name-to-title-to-company match, tracking member IP addresses, and leveraging member feedback to identify fake accounts at scale. Accordingly, every new user registration attempt would be evaluated by a machine-learned model that gives an abuse risk score. Signup attempts with a low abuse risk score would be allowed to register right away, while attempts with a high abuse risk score would be prevented from creating an account. Attempts with medium risk scores would be challenged by LinkedIn's security measures to verify that they are real people. LinkedIn also reportedly uses verification badge icons. EU Members may voluntarily verify their identity through LinkedIn's verification partner, Persona, with hard-to-falsify documents like E-passports. In jurisdictions where it is legally allowed, LinkedIn's identity verification partners independently use liveness checks to confirm that the picture in the ID document submitted to the partner matches the member's face.
Pinterest	No specific identity verification measures are reported by Pinterest. Pinterest reports that it requires users to submit government IDs and/or a selfie to a third-party partner for age verification when a user who previously entered their age as under 18 attempts to edit their date of birth. Per the platform, this check does not apply for initial account creation.
Pornhub	<u>Uploader account</u> Pornhub reports that every new uploader is required to undergo identity verification with a third-party identity verification provider, which requires them to submit a government-issued ID, which is authenticated by the provider, and to conduct a liveness test to ensure the user's likeness matches the government-issued ID and they are the same person. Pornhub states that the liveness test is designed to ensure that the person is alive and real. The platform also reports that content partners are required to go through a KYC process to validate their identity and business, and that all content partners go through an annual audit where they are required to provide documentation for a random selection of their content.
	<u>Personal account</u> Pornhub reports that it allows anonymous user profiles and does not require account creation to access content.

Designated service	Measure description
Snapchat	Snapchat reports that users are prompted to provide their first name, last name (optional), birthday, and username for account creation, as well as a phone number and/or email. Snapchat reports that it is exploring age estimation and identity verification methods, considering third-party technologies including biometrics, ID scans and financial transaction methods. These methods have not been implemented yet and are primarily reported in relation to minor protection risks.
Shein	No information is provided by Shein on identity verification for the creation of personal user accounts.
Temu	No information is provided by Temu on identity verification for the creation of personal user accounts.
TikTok	TikTok reports that self-declaration is used for initial account creation, and that, for appeals concerning age-gating measures, users can use proof of age to appeal a determination that they do not meet the Minimum Age Requirement by: (i) providing a selfie with ID; (ii) providing a photo with a trusted adult; (iii) using credit card authorisation (if an Adult User); or (iv) using AI facial age estimation via a third-party service provider. These methods would only apply to appeal procedures, not account creation.
Wikipedia	No specific identity verification measures are reported by Wikipedia.
X	X reports that it allows anonymity, valuing the ability to create anonymous or pseudonymous accounts.
XNXX	<u>Uploader account</u> XNXX reports that users who upload videos via XNXX are not required to verify themselves. However, for uploading tagged content, uploader verification would be required. This verification can be completed through alternative upload channels and may include several procedures depending on the chosen route. Reportedly, the verification process may require submission of an official ID document and content samples demonstrating that the uploader is the same person appearing in the video. Verification checks would confirm the uploader's name, date of birth (age verification), and consent and ownership of the content. XNXX also states that, in other cases, verification would involve a profile picture and a video upload, confirming the visual content matching (authorship).
	<u>Personal account</u> XNXX reports that for regular users, those who watch or comment on videos, verification is limited to basic email validation upon account registration – which is, however, not required -, and that this approach would confirm authenticity while maintaining accessibility for non-uploading users. XNXX states that the process of account creation includes an age declaration and the user's agreement with the Terms of Service (ToS).
XVideos	XVideos reports that its ToS prohibits the use of fake identities or the impersonation of individuals or entities. XVideos does not mention identity verification measures.
Zalando	No information is provided by Zalando on identity verification for the creation of personal user accounts.

KYBC requirements

Table 16 - Overview of KYBC measures as reported by the designated services[1408]

Designated service	Measure description
AliExpress	AliExpress reports that the verification process for seller onboarding includes validating their legitimacy against official databases (including the EU VAT Information Exchange System for European sellers, and a Chinese system for China-based sellers) and reviewing the company's documentation. Accordingly, sellers must submit business registrations and license details, legal representative information, corporate structure documentation, and funding account data. AliExpress also reports that seller onboarding controls include an automated vetting system, and that seller accounts are verified to detect any similarities between new applicants and sellers previously banned from the marketplace. AliExpress notes that it enforces a limit on the number of stores per legal entity, and if a store is terminated for breaching the platform's Terms and Conditions (T&Cs), the entity would not be allowed to reopen it or create new ones. The 2025 Independent Audit of AliExpress provided a positive conclusion on the platform's implementation of trader traceability requirements.[1409]
Amazon Store	Amazon indicates that it verifies the identities of potential sellers through a combination of automated models and human review: sellers must open an account with Amazon Payments Europe (APE), an authorised electronic money institution established in Luxembourg. Registration with APE requires identity and background checks through the submission of government-issued IDs, tax information, business license, phone number, address, bank account number, bank routing number, and a chargeable credit card. Amazon reports that it also employs automated identity detection methods, including document forgery detection and image and audio-video verification. Amazon indicates that it also relies on an in-person verification program, which requires all prospective sellers to have one-on-one conversations with an Amazon employee to verify their identity and documentation. As an alternative, sellers can rely on instant identity verification processes through a complete live video check that demonstrates the physical possession of identification documents. The 2025 Independent Audit of Amazon Store provided a positive conclusion on the platform's implementation of trader traceability requirements.[1410]

[1408] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

[1409] FTI Consulting, Independent Audit of AliExpress – Article 37 of Regulation (EU) 2022/2065 (Digital Services Act), available at: https://www.dropbox.com/scl/fi/8mn8wigchllrxpp4kypkz/2025-Audit-Report.pdf?rlkey=lntmlgoo5evtvxo6qa3s6xeuh&st=p1l4ehg7&e=1&dl=0.

[1410] KPMG, DSA Assurance Report – Independent practitioner's assurance report concerning Regulation (EU) 2022/2065, the Digital Services Act (DSA), available at: https://www.dropbox.com/scl/fi/4weflzsc8jqs2zhr0xyq1/eu-dsa-audit-report-amazon-2025.pdf?rlkey=p2xi6la8ifh2npf6ofi9rjosi&st=tlzb82dk&e=1&dl=0.

Designated service	Measure description
Apple AppStore	Apple App Store reports that developers must register as Apple Developers before publishing their apps through the App Store; in doing so, prospective developers would be required to provide identity information and verify it with government-issued identity documents. Apple indicates that it conducts identity verification and other risk-based checks to identify developers whom it considers unlikely to comply with the Apple Developer Agreement (the "ADA") and DPLA. Apple uses submitted developer data as a secure hash to scan for and block developers attempting to register multiple accounts. Reportedly, the World Wide Developer Relations team conducts a screening intended to prevent fraudulent developers from enrolling, including verifying developer identity, enrolment country, and financial information, as well as automated checks against existing and terminated developer accounts to ensure that developers who have previously committed or show indicators of intending to commit serious breaches of the App Store T&Cs do not re-enter the platform. Apple also indicates that it obtains information from developers who specify that they meet the definition of a "trader", including (a) the developer's name, address, telephone number and email address; (b) identification documents; (c) payment account details; (d) registration information; and (e) self-certification by the developer committing to only offer products or services that comply with applicable EU law. This detail would then be published on the trader's app product page. The 2025 Independent Audit of Apple AppStore generally provided a positive conclusion on the platform's implementation of trader traceability requirements.[1411] According to the Independent Audit Report, shortcomings in the implementation of Article 30(7) DSA, whereby several developers had apps available on the App Store without the information referred to in Article 30(1) DSA, were remedied on 17 February 2025.[1412]
Bing	No specific KYBC measures are reported by Bing. Bing does not allow consumers to conclude distance contracts with traders.
Booking.com	Booking.com reports that it carries out due diligence on its supply partners, including verification methods aimed at verifying the location of properties. Reportedly, these include using machine learning models to identify fraudulent properties. The 2025 Independent Audit of Booking.com provided a positive conclusion on the platform's implementation of trader traceability requirements, with comments recommending the introduction of a monitoring system with manual periodic reviews of traders.[1413]
Meta designated services	Facebook and Instagram note that they maintain verification processes for official accounts related to elections, commerce, and paid content. Reportedly, accounts may be reviewed before being able to post content and interact with users. No further information on these verification processes is provided by the platforms. Facebook and Instagram do not allow consumers to conclude distance contracts with traders.
Google Play	Google Play reports that it verifies the identity of developers by requiring them to provide a D-U-N-S number (nine-digit identifiers used to verify businesses), alongside requirements such as legal name and address, email, and a Google payment profile. Google Play also

[1411] EY, Independent Audit on the App Store, available at: https://www.dropbox.com/scl/fi/htdwuqum9fljh7mw7fjkn/20251119_app-store_reasonable-assurance-report_non-confidential.pdf?rlkey=khz719r2fc8zn3rxaesfmqp4y&st=1xb8hi68&e=1&dl=0.

[1412] ibid.

[1413] Deloitte, Booking.com B.V. Digital services Act (DSA) Assurance Report, available at: https://www.dropbox.com/scl/fi/pct8bi29kykqq1tda58ct/2025-Audit-report.pdf?rlkey=t3mjd9dqmuer2rx4em6fyswwk&st=b7ohtnyo&e=1&dl=0.

Designated service	Measure description
	indicates that prospective developers may be required to submit official organisation documents to help verify their information; reportedly, developers with unverified bank accounts have their content removed from the platform. As per the 2025 Independent Audit, Google reports that it considers that Google Play does not meet the definition of an online platform allowing consumers to conclude distance contracts with traders.[1414]
Google Shopping	Google Shopping reports that it reviews and verifies merchant identity-related signals, including VAT information and that, in some cases, it requires explicit identity verification. Reportedly, Google Shopping also uses location, social media presence, and third-party consumer research sources to mitigate the risk of fraudulent business information. As per the 2025 Independent Audit, Google reports that Article 30 DSA does not apply to Google Shopping due to the nature of the services offered by the platform (redirecting users to external sites to make purchases).[1415] As all sales are made on the external sites, not on the Google Shopping platform, Google maintains that there are no traders concluding distance contracts with consumers.[1416]
Other Google designated services	No specific KYBC measures are reported by Google. Other Google VLOPs and VLOSE do not allow consumers to conclude distance contracts with traders.
LinkedIn	No specific KYBC measures are reported by LinkedIn. LinkedIn does not allow consumers to conclude distance contracts with traders.
Pinterest	No specific KYBC measures are reported by Pinterest. Pinterest does not allow consumers to conclude distance contracts with traders.
Pornhub	No specific KYBC measures are reported by Pornhub. Pornhub does not allow consumers to conclude distance contracts with traders.
Shein	Shein reports that Sellers must complete an onboarding and verification phase before they can be listed on the Marketplace. During this phase, prospective Sellers submit an initial online application involving the sharing of detailed information to become a trader on the Marketplace. Shein indicates that it conducts an initial screening of the application before issuing approved Sellers with login credentials to become onboarded; this consists of both verifying the information provided and reviewing the Seller's past activity. Reportedly, this is followed by a 'Know Your Customer' ('KYC') process, which involves ensuring compliance with regulatory requirements and enhancing the security of financial transactions effected through the Marketplace. Sellers would then be required to provide information about their business, such as business registration documents, tax identification numbers and contact details of their key management. Shein notes that once KYC has been passed, Sellers are then fully onboarded and can start listing their products on the Marketplace. Shein also reports that, if a Seller makes any changes to its information, company structure, or business scope, this information would be verified in real-time

[1414] EY, Independent Audit on Google Play – Digital Services Act, available at: https://www.dropbox.com/scl/fi/81133n2f15wdsbmu8gx7n/2025-Audit-report.pdf?rlkey=7n715t6euz6myjwdq0yj4256o&st=18p4fs82&e=1&dl=0.

[1415] EY, Independent Audit on Google Shopping – Digital Services Act, available at: https://www.dropbox.com/scl/fi/ti6dfeps05kwr5207h69m/2025-Audit-report.pdf?rlkey=7vfrm35jqjsle8pxgsmppy493&st=vylqyh0o&e=1&dl=0.

[1416] ibid.

Designated service	Measure description
	for accuracy. If the Seller does not pass KYC with the new information, Shein reports that it will suspend the account until all necessary information has been provided and verified. The 2025 Independent Audit of Shein provided a positive conclusion on the platform's implementation of trader traceability requirements.[1417]
Snapchat	No specific KYBC measures are reported by Snapchat. Snapchat does not allow consumers to conclude distance contracts with traders.
Temu	Temu reports that during seller onboarding, it collects, stores and processes user information beyond basic contact details, including business registration documents, legal representative identification, and other critical information necessary for traceability, and that this process is followed by a verification procedure. Reportedly, automated screening first analyses submitted information for irregularities and obvious errors: if an inconsistency is identified, the application is then further progressed to manual review for evaluation. This verification procedure includes cross-referencing the provided information with third-party databases to verify their reliability and completeness. Furthermore, Temu reports that it screens all prospective traders against its internal 'Trader Blocklist', which aggregates sanction lists from global regulatory authorities to prevent high-risk sanctioned entities from gaining access to Temu. Temu also indicates that it maintains a separate onboarding restriction list to block identified rogue traders found to have engaged in deliberate or repeated misconduct from re-entering its platform. Accordingly, attempts to gain access through false, duplicate, or incomplete registrations are blocked through the initial vetting process. Following onboarding, Temu reports that it implements continuous monitoring, reviewing trader information to ensure it is accurate and up to date: when changes occur or key details approach expiration, traders are notified and required to update their records accordingly. Temu indicates that failure to provide updates information results in enforcement actions, including suspension of their ability to sell to the EU market. The 2025 Independent Audit of Temu provided a positive conclusion on the platform's implementation of trader traceability requirements.[1418]
TikTok	TikTok reports that it implements the following measures in relation to Seller Account verification: (i) seller onboarding that includes verification of sellers' personal and corporate identity and address, applicable regulatory checks and use of information from third-party risk vendors; (ii) "block lists" to prevent sellers previously blocked for fraudulent behaviour or repeated policy violations from rejoining; (iii) creator controls that include ID validation and verification of age checks before creators can share Shop Content.

[1417] Deloitte, DSA Assurance Report – Independent practitioner's assurance report concerning Regulation (EU) 2022/2065, the Digital Services Act (DSA), available at: https://www.dropbox.com/scl/fi/vaxfl4vttxcg8wj78feb4/2025-Audit-Report.pdf?rlkey=vc6iilli3101zyolwrv5y0w1f&st=qmfkmndl&e=1&dl=0.

[1418] EY, Independent Audit on TEMU, available at: https://www.dropbox.com/scl/fi/buv4tarf7mkf11vq5ec5n/DSA-Audit-Report-2025.pdf?rlkey=qtogc37szpbj32eredokjwujx&st=6gl4n32w&e=1&dl=0.

Designated service	Measure description
	The 2025 Independent Audit of TikTok provided a positive conclusion on the platform's implementation of trader traceability requirements.[1419] The Independent Audit notes that TikTok did not provide evidence demonstrating the design, implementation, and operating effectiveness of General IT Controls for the systems related to trader traceability.[1420] The Independent Audit reportedly performed additional substantive procedures to assess these aspects.
Wikipedia	No specific KYBC measures are reported by Wikipedia. Wikipedia does not allow consumers to conclude distance contracts with traders.
X	No specific KYBC measures are reported by X. X does not allow consumers to conclude distance contracts with traders.
XNXX	No specific KYBC measures are reported by XNXX. XNXX does not allow consumers to conclude distance contracts with traders.
XVideos	No specific KYBC measures are reported by XVideos. XVideos does not allow consumers to conclude distance contracts with traders.
Zalando	Zalando reports that its platform is only available for registered companies and professionals to offer products and provider-related content, and that each partner is subject to a due diligence process and goes through an onboarding process containing KYC (Know Your [Business] Customer) checks. The 2025 Independent Audit of Zalando provided a positive conclusion on the platform's implementation of trader traceability requirements.[1421]

[1419] KPMG, DSA Assurance Report - Independent practitioner's assurance report concerning Regulation (EU) 2022/2065, the Digital Services Act (DSA), available at: https://www.dropbox.com/scl/fi/nldbvg99c59xrfmvja8qm/DSAAssuranceReport-TikTokTechnologyLimited-2025.pdf?rlkey=or3n1vnu5ocfub7oi3lejrf88&st=qgo9y1gj&e=1&dl=0.

[1420] ibid.

[1421] Deloitte, Independent Practitioner's Assurance Report on Zalando SE's compliance with the Digital Services Act, available at: https://www.dropbox.com/scl/fi/n8dnm429o1r17uwbc7lbv/2025-Audit-Report.pdf?rlkey=5dq7gcxsymv1kx6kvrof03xrw&st=8msssumh&e=1&dl=0.

Ad placement requirements

Table 17 - Overview of ad placement requirements as reported by the designated services[1422]

Designated service	Measure description
AliExpress	AliExpress reports that admission standards are applied to sellers wishing to participate in promotions as part of the advertising system, including review of moderation history and penalty records. AliExpress indicates that the content of advertisements is run through a detection system pre-publication. Reportedly, products and sellers that are blocked or identified as high-risk are automatically excluded from the advertising pool. AliExpress also notes that advertisement content for Pay-Per-Click is only published after passing a risk control review that combines algorithmic and manual review. The platform states that any associated advertisements are blocked when a product is delisted as part of product control measures.
Amazon Store	Amazon Store reports that advertising content mainly appears as Sponsored Products and Sponsored Brands placements, which respond to customer search queries or product detail page context. Amazon indicates that Seller Account identity verification measures also apply to advertisements. It reports that ad moderation includes automated review of all visible ad elements (images, titles, descriptions), human review, and blocking of specific product categories from advertising. Amazon also indicates that it regularly audits live ads to identify any potentially non-compliant ads, using the findings to improve its automated moderation tools and the training processes for human reviewers. Amazon claims that it proactively detects and acts against advertisers that breach its advertising policies.
Apple App Store	Apple App Store reports that certain app categories face promotion restrictions managed by the Apple Ads team, potentially requiring proof of specific permits or licences. Apple App Store's Report does not mention specific measures for identity verification of advertisers. Apple states that the Apple Ads team reviews promoted app placement for content, imagery, and promotion category classification, and that promoted apps, which are already approved for the App Store, undergo further review against Apple Ads terms and conditions. The Ads team also reportedly monitors account and advertiser actions for signs of potential misconduct and handles complaints relating to Apple Ads advertising.
Bing	Bing's report states that Microsoft Advertising uses a multi-tiered detection system combining machine learning models, heuristic rules, and manual reviews to moderate ad content. The report also notes that Advertiser Identity Verification (AIV) processes require advertisers to prove their legal identity before running ads. Bing indicates that content policies prohibit misleading, deceptive, and fraudulent ad content, and that it has detection models and rules that apply at the advertiser-level and at the particular ad level. Bing reports that some of the models that apply at the advertiser-level include: • Payment fraud detection: This model triggers when the advertiser adds a payment instrument.

[1422] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

Designated service	Measure description
	• Purchase risk model: This model triggers upon billing the advertiser to determine whether to try to make the charge or block the advertiser. • Behavioural risk model: This model looks at various features of an advertiser's account or campaign(s), such as the ad text, keywords, budgets, account age, account structure, attributes of the payment instrument, individuals associated with the account, devices from which the advertiser is accessing the system, etc., to determine the risk of an advertiser being fraudulent. This model runs when the advertiser makes any changes to their ad campaigns (ads/keywords/budgets, etc.). • LLM-based spoofing detection: One of the large categories of fraud is where advertisers pretend to be a legitimate site (e.g., trying to deceive users into believing that an ad leads to the official website of a bank). Bing has an LLM-based approach looking at advertiser demand to try and predict if the advertiser is engaging in this behaviour. Bing states that Relevance and Quality Policies ensure ads are legal, relevant, and not misleading. The search engine also notes that Bing users can also report advertising for takedown through the "feedback" function, and that detection of violative ad content covers ad text, images, extensions, product feeds and components, landing pages, URLs, keywords, and targeting settings.
Booking.com	Booking.com states that it does not derive its core revenues from ad products that require user-level targeting.
Meta designated services	Meta reports that its Advertising Standards, as applicable to Facebook and Instagram, concern allowed ad content, review processes, and transparency requirements. Moreover, it states that Special Ad Categories (employment, housing, financial products) impose additional requirements, including limited audience selection tools. Facebook and Instagram note that they maintain additional verification processes for official accounts related to elections, commerce, and paid content, and that accounts may be reviewed prior to being able to post content and interact with users. Meta describes that all ads are automatically reviewed against its Advertising Standards before launching on Facebook or Instagram; automated review mechanisms analyse ads, sponsored Marketplace listings, for-sale posts, and other commerce listings before they go live. Meta notes that these mechanisms block policy-violating content using keyword detection and machine-learning models, and that it also uses human reviewers to improve and train its automated systems, and in some cases, to manually review ads. The company describes a 24-hour hold on distribution that applies while ads are under review. Meta also notes that some ads can be selected for reactive review after they are published – this would happen for various reasons, including if a user reports the ad as potentially violating. The entire ad would be reviewed to determine if it violates Meta's Advertising Standards.
Google designated services	Google reports that its advertising policies cover prohibited content (e.g., counterfeit goods, dangerous products), prohibited practices (e.g., misrepresentation, circumvention of ad review), restricted content requiring advertiser certifications (e.g., alcohol, gambling, financial services, political content), and editorial and technical standards. Google notes that its ad review processes cover the content of ads, including the ad content (e.g., text, images, video, audio of ad), targeting (e.g., search keywords), and destination (e.g., advertiser's web page). Accordingly, ads that do not comply with Google policies are disapproved and are not able to run until the policy violation is fixed and the ad is reviewed again. Google also notes that users can report ads that they find inappropriate or which they believe may violate the law or Google policies. Google states that its generative AI content is held to the same set of content standards, reviews, and enforcement for any policy violations. Furthermore, it states that all images generated by Google Ads include mechanisms that allow them to be identified as generated, such

Designated service	Measure description
	as open-standard markup that will surface on tools like Google Image Search, as well as SynthID, which is an imperceptible digital watermark that's resistant to manipulations of the image, such as screenshots, filters, and compression.
LinkedIn	LinkedIn reports that its advertising function consists of fully integrated first-party advertising on LinkedIn with a focus on "business-to-business" marketing; there are four types of ads on LinkedIn: Sponsored Content, Text Ads, Sponsored Messaging, and Dynamic Ads. No specific measures for identity verification of advertisers are described by LinkedIn in its Report. LinkedIn also reports that it automatically evaluates advertisements against platform policies at creation. These policies include, among other things, prohibitions on political advertisements; policies that limit healthcare-related advertisements to come from certified retailers and that limit distribution to jurisdictions where such advertisements are legal; and policies that prohibit discrimination based on protected characteristics. LinkedIn indicates that it relies on a three-layered detection process, involving automatic and proactive prevention, automatic and human-led detection, and user reporting.
Pinterest	Pinterest describes its Advertising Guidelines as covering prohibited and restricted ad categories (e.g., drugs, sensitive content, tobacco, alcohol, gambling, political campaigns, adult content), including country-specific rules. Pinterest reports that it enforces identity verification for ads only in relation to shopping ads, placed by merchants. At the account level, Pinterest reports that it reviews every business wishing to become a verified merchant on Pinterest. Pinterest indicates that it uses a mixture of manual review and other controls to enforce its Advertising Guidelines. In addition to the manual review of ads, the platform also declares that it uses tooling to auto-review duplicate ads. Pinterest indicates that it enforces a separate policy for shopping ads (ads that directly link to a shopping experience through a merchant's website or app). Accordingly, these ads are not manually reviewed prior to being served, but are subject to additional controls including user reports, hide-triggered reviews, and machine learning models detecting prohibited products. Pinterest holds that once identified, these will ads are manually reviewed and taken down if they are confirmed to violate its Advertising Guidelines.
Pornhub	Pornhub states that its advertising is subject to the same controls as the other content it hosts, including automated moderation tools and human moderation before publication. Pornhub declares that it allows advertising from NGOs who provide services to help change problematic user behaviour. No specific measures for identity verification of advertisers are described by Pornhub in its Report. Pornhub also indicates that all users (logged in or not) can report adverts that they believe to contain illegal, inappropriate or copyright material.
Shein	Shein states that it does not allow seller advertising. Whilst some promotional activity takes place on the marketplace, the platform reports that this relates exclusively to listed products, as Shein does not allow third-party advertising.
Snapchat	Snapchat reports that its advertising policies prohibit ads displaying information that violates the law or causes certain harms. No specific measures for identity verification of advertisers are described by Snapchat in its Report. Snapchat also indicates that ads are reviewed pre-publication through a combination of automation and human review. Snapchat also reports on mechanisms for users to hide and report advertisements that violate its policies or the law. The platform also states that it monitors ad rejection, reporting and enforcement data to monitor the effectiveness of its approach.

Designated service	Measure description
Temu	Temu reports that it does not host on-platform advertising, but it implements an Affiliate and Influencer Programme (A&I Programme) for off-platform promotional activities. Accordingly, the A&I Programme extends the reach of product listings on Temu to users of third-party platforms. Temu describes that any product is subject to standard content moderation before it can be considered for a promotion. As such, in case a product in a promotional slot is identified as infringing (e.g., via user reports), the immediate reactive step described by Temu is to remove it from the promotion, in addition to taking down the product listing itself. An incident of this nature would trigger a reactive review of the curation process to identify and rectify any gaps that allowed the product to be selected. In addition to the measures applied to on-platform promotions (content moderation, internal curation process, user reports), Temu also indicates that its Affiliate Policy and Influencer Policy bind all participants to the A&I Programme to a code of conduct that sets rules for their activities.
TikTok	TikTok indicates that its Advertising Policies and Community Guidelines prohibit inaccurate, misleading or false content that may cause significant harm to individuals or society. Moreover, TikTok's Advertising Policies restrict certain industries (e.g. Healthcare and Pharmaceuticals, Financial Services and Products and Weight Management) from advertising to Younger Users. No specific measures for identity verification of advertisers are described by TikTok in its Report. TikTok's Advertising Policies stipulate that documents may be required to verify that the business or organisation is eligible to advertise on TikTok.[1423] TikTok reports that all ads are subject to automated pre-publication review, which is designed to flag ads that may violate TikTok's Advertising Policies. TikTok also mentions that the automated moderation of ads is supplemented by a number of 10 proactive and reactive detection measures, including risk monitoring, further review, user reports and regulatory or legal escalations. TikTok states that it conducts regular monitoring of potentially violative ads in high-risk areas and uses information gathered to improve its automated moderation measures and mitigate concentrated areas of risk.
Wikipedia	Wikipedia reports that it does not allow ad placements.
X	X reports that its Ads Policies prohibit the promotion of illegal products and services. X also reports that it does not serve any ads to users under the age of 18 in the EU, as of August 2023. The platform also states that logged-out users are not served ads. X reports that an active X Premium subscription is required to be eligible to run ads on X, and that it conducts sanctions screening on all verified Premium users to ensure that X does not disburse payments to individuals on sanctions lists. If any users are confirmed to be sanctioned, X states that it implements an indefinite restriction on their access to all monetisation features. X describes that it employs machine learning models and business logic such as denylist terms to proactively detect violative ads pre-publication. Accordingly, human reviews are used to verify automated detections, which can also be initiated due to user reports. The platform declares that users can report ads for deceptive and fraudulent content and illegal products and services through in-app reporting or the X Ads web form, and that detected ads are removed or restricted per its Ads policies. X also states that community Notes can be added to X Ads to help ensure the veracity of the advertiser's claims and allow access to more information.

[1423] TikTok Business Resource Center, Advertiser Account Policy (2025), available at: https://ads.tiktok.com/resources/help/article/actor-policy.

Designated service	Measure description
XNXX	XNXX reports that the Advertisers Certification Program requires advertisers to meet eligibility criteria, undergo formal assessment, and submit to periodic compliance reviews. It also states that certified advertisers are reviewed periodically to confirm continued compliance, and that any detected violations may result in removal of certification, suspension of campaigns, or termination of the advertising account. XNXX reports that all ads are manually reviewed pre-publication against internal rules using antivirus scanners, URL analysers, VPNs, and translation tools, and that prohibited categories include non-consensual content, violence, malware, phishing, political ads, and others. The platform also indicates that EU/UK/California-targeted ads undergo additional cookie compliance checks. XNXX states that approved ads are subject to continuous scanning, with a tiered violation process (labelling, decline, suspension, or permanent ban)
XVideos	No specific measures for identity verification of advertisers are described by XVideos in its Report. XVideos reports that all ads undergo pre-publication review by trained personnel, checking for compliance with legal requirements and platform policies, including misleading claims, deceptive promotions, undisclosed sponsorships, and content appropriateness.
Zalando	Zalando reports that its advertising features fashion, beauty, and lifestyle content through sponsored products on the marketplace, and that advertiser identity verification overlaps with its KYBC processes.

Labelling AI-generated content

Table 18 - Overview of how designated services report to detect and label AI-generated content[1424]

Designated service	Measure description
AliExpress	No specific measures for detecting or labelling AI-generated content are described by AliExpress in the Report. AliExpress acknowledges the necessity of developing detection algorithms for AI-generated content (AIGC).
Amazon Store	No specific measures for detecting or labelling AI-generated content are described by Amazon Store in the Report.
Apple App Store	No specific measures for detecting or labelling AI-generated content are described by Apple App Store in the Report. The Report acknowledges that a range of apps on the App Store have AI features or can be used to generate AI imagery. Apple states that, in addition to the Guidelines applicable to all apps, those apps with user-generated content (UGC) are subject to a range of controls, including the requirement to include a method for filtering objectionable material from being posted to the app, a mechanism to report offensive content and secure timely responses, the ability to block abusive users, and publication of contact information for the developer.
Bing	Bing describes that it offers content-generation features that use AI, and that these features include content credentials and a pixel-based watermark on generated images. Accordingly, the Watermark complements Bing's content provenance technology to help ensure an AI-generated image's integrity and traceability. Bing reports that it has implemented safeguards, such as C2PA-enabled signing and the Content Credentials tool, to help review and verify the authenticity of digital content. Bing indicates that it displays prominent disclosures and in-product notices when users are engaging with AI-generated content. For example, in Copilot Search, an information icon near the feedback buttons alerts users that the response was generated by AI. Bing explains that hovering over this icon reveals a plain-language explanation, with links to more detailed documentation. These disclosures are reportedly written at a fifth-grade reading level to ensure they are accessible to young users and audiences of varying digital fluency. To support informed engagement and reduce manipulation, Bing reports that it has also introduced content integrity as a Service, a system that uses digital credentials and cryptography to authenticate the origin of media. Bing states that this helps users trust that the images or media they are seeing have not been tampered with, and that they come from verified sources. Bing also refers to its Terms and Conditions for Users, found within the Bing Image Creator Terms, as applied to Civic Discourse and Electoral Processes. This policy prohibits use of the service to engage in activity that is false or misleading; to attempt to create or share content that could mislead or deceive others, including, for example, creation of disinformation, or deceptive impersonation; to remove or alter content credentials or other provenance methods, marks, or signals that indicate that the Creations were generated by the service; or to otherwise attempt to mislead others about whether the Creations were generated by the service.
Booking.com	No specific measures for detecting or labelling AI-generated content are described by Booking.com in the Report.

[1424] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

Designated service	Measure description
Meta designated services	Facebook and Instagram report implementing transparency labelling, such as utilising synthetic data to improve labelling performance against AI content and providing signals to human reviewers when we know something is created by GenAI. Meta reports that it maintains tools to automatically label photorealistic images created using MetaAI and posted on Meta platforms, and that its GenAI Trust team uses a tool to label and identify images exhibiting certain industry-standard AI technical identifiers that users post to Facebook that were generated using MetaAI. Meta also indicates that its AI Safety Team implements and adapts Meta's proactive detection technology to enable identification of potentially violating GenAI prompts and responses. Accordingly, proactive detection systems are trained with synthetic data to identify and improve performance against GenAI content on Meta's platforms. Additionally, Facebook and Instagram indicate implementing targeted system and product measures to address the risk of propagating false or misleading GenAI content, including labelling of AI-generated or edited content, building a feature for people to disclose when they share certain AI-generated media so it can be labelled, building invisible markers to help detect deep-fakes, and requiring advertisers running ads on social issues, elections, or politics to identify digitally altered and/or AI-generated content. Facebook and Instagram report that in May 2024 they began labelling a wider range of video, audio, and image content based on detection of industry-standard AI-image indicators. Accordingly, if Meta determines that digitally created or altered image, video, or audio content creates a particularly high risk of materially deceiving the public on a matter of importance, it may add a more prominent label, so that people have more information and context.
Google designated services	Google reports that it has launched SynthID, a tool for watermarking and identifying AI-generated content. Google states that this technology embeds a digital watermark directly into the images, text, audio, and video generated with Google's AI tools in a way that is imperceptible to the human eye but detectable for identification. Google states that it is not exposing SynthID labels to users, but that the ability to identify computer-generated content is one of the methods it uses to promote high-quality information. In addition, Google claims that any content published by Lyria, Google's AI music generation model used by YouTube, will be watermarked with SynthID. Similar to how it handles images, SynthID embeds a watermark into AI-generated audio content that is inaudible to the human ear and doesn't compromise the listening experience. Google states that this watermark is designed to maintain detectability even when the audio content undergoes modifications such as noise additions, compression, or speeding up and slowing down the track. Google also reports that it is a steering committee member of C2PA and uses C2PA Content Credentials across its range of generative media tools. YouTube claims that any content published on YouTube that was created on Veo, Google DeepMind's video generation model, will be embedded with a watermark using SynthID. YouTube claims that users will also be able to identify these creations through a content label that clearly communicates if a piece of content was generated using AI. Google also reports that creators on YouTube are required to disclose synthetic content when it's realistic, meaning that a viewer could easily mistake what's being shown with a real person, place, or event, and the alteration is not inconsequential. To that end, Google indicates that creators are provided with a tool in Creator Studio to label their videos as synthetic prior to sharing them. When creators fail to apply the

Designated service	Measure description
	label, and YouTube claims being able to confirm that the content is synthetic or manipulated and seems realistic, YouTube may apply a label.[1425] Google reports that it developed identification technology that will be meant to allow its partners, creators, actors, musicians, and athletes to automatically detect AI-generated content using their faces that constitutes misuse based on Google's Community Guidelines.
LinkedIn	LinkedIn indicates that it has also adopted the C2PA to include metadata labelling, including data about whether content is created using AI, on content containing the C2PA technology. LinkedIn describes implementing a set of guidelines to ensure transparency and clear labelling across all AI-driven tools, products, or features. Accordingly, this approach would involve consistent iconography and language throughout the member experience, context-appropriate labelling to distinguish AI from non-AI-generated content, adherence to legal and trust guidelines to avoid deceptive practices, and the inclusion of feedback mechanisms for GenAI experiences. LinkedIn also indicates that content containing the C2PA Content Credentials will be automatically labelled on LinkedIn, with users seeing the "Cr" label. As such, by clicking the label, users would be able to trace the origin of the AI-created media, including the source and history of the content, and whether it was created or edited by AI. LinkedIn also reports that it is investing in AI technologies such as advanced network algorithms that detect communities of fake accounts through similarities in their content and behaviour; computer vision and natural language processing algorithms for detecting AI-generated elements in fake Profiles such as deepfakes; anomaly detection of risky behaviours; and deep learning models for detecting sequences of activity that are associated with abusive automation.
Pinterest	Pinterest reports that it labels content when metadata indicates it was created or modified by AI, and that its content moderation tools do not distinguish between harmful content that is manipulated or edited and harmful content that has not been manipulated. Pinterest states that its content moderation tools work to identify and action all policy-violating and harmful content regardless of how it was created.
Pornhub	No specific measures for detecting or labelling AI-generated content are described by Pornhub in the Report.
Shein	No specific measures for detecting or labelling AI-generated content are described by Shein in the Report.
Snapchat	Snapchat reports using a range of methods to notify users that they are interacting with or viewing AI-generated content. These include: • The sparkle icon displayed alongside features or outputs powered by AI. • Context Cards or disclaimers that explain when a feature is AI-driven. • On-screen tooltips or labels that appear within relevant features like Dreams and AI Snaps • In some cases, visible watermarks, such as a Snap Ghost with sparkles, are added to exported or saved images created using generative AI tools. Snapchat indicates that, when users export AI-generated images to their Camera Roll, these images will include a watermark indicating they were created using Snap's AI-powered tools.
Temu	No specific measures for detecting or labelling AI-generated content are described by Temu in the Report.

[1425] YouTube Help, Disclosing use of GenAI content, available at: https://support.google.com/youtube/answer/14328491#zippy=%2Cexamples-of-content-creators-dont-have-to-disclose%2Cexamples-of-content-creators-need-to-disclose.

Designated service	Measure description
TikTok	TikTok describes working with industry groups and civil society to detect undisclosed AIGC. TikTok reports that it participates in the C2PA, using the C2PA Content Credentials to detect AIGC at scale when content with that metadata is uploaded to the Platform. TikTok declares that its capacity to detect AIGC is reinforced by its content moderation systems for content violative of TikTok's Community Guidelines, external partner reports, internal teams who identify instances of violative use of AIGC, manual reviews of trending or popular content, and targeted proactive sweeps.
Wikipedia	No specific measures for detecting or labelling AI-generated content are described by Wikipedia in the Report.
X	No specific measures for detecting and labelling AI-generated content are described by X in the Report. X holds that any AI-generated content is subject to X's Rules, and that it enforces its policies irrespective of the source of creation or generation of such content. X reports that when it comes to harmful and illegal content and behaviour, its priority is to catch it and take action regardless of whether or not it has been generated using AI.
XNXX	No specific measures for detecting or labelling AI-generated content are described by XNXX in the Report.
XVideos	XVideos reports that it is currently investing in research on generative AI technologies to understand emerging threats better, and that its Terms of Service prohibit AI-generated content the substance of which would violate its policies.
Zalando	No specific measures for detecting or labelling AI-generated content are described by Zalando in the Report.

Automated detection systems

Table 19 - Overview of automated detection systems as reported by the designated services[1426]

Designated service	Measure description
AliExpress	AliExpress describes that automated moderation systems analyse both listing images and text to detect counterfeit or illegal products. The platform states that automated systems also monitor transaction and logistics patterns, including abnormal order volumes, suspicious delivery declarations, invalid logistics information, and indicators of fake shipments, to detect fraud and seller manipulation. Further, it indicates that machine-learning systems analyse review activity using signals such as account linkages, sign-in behaviour, review histories, and other indicators associated with coordinated review manipulation. Another detection system described by AliExpress focuses on risk-behaviour indicators used during listing moderation and the platform's efforts to detect deliberate mis-categorisation of prohibited products through combined image and text analysis. AliExpress reports that the content of AliExpress' Instant Messaging feature is moderated through a combination of pre-publication and post-publication filtering, and that images and videos are subject to post-publication review, while reviews and Q&A content are screened through automated filtering.
Amazon Store	Amazon Store describes that image and text analysis technologies are used to detect counterfeit, infringing, fraudulent, or otherwise non-compliant products. The platform indicates that automated product listing controls use keyword-based algorithms and machine-learning models to identify and remove product offers that may breach safety, compliance, or platform policies, with its models analysing signals relating to products, brands, offers, and sellers. Amazon reports that in 2025 it introduced "SENTRIX", an AI-powered system designed to identify and facilitate the removal of malicious websites impersonating Amazon services.[1427] Accordingly, the system would analyse both textual and visual elements, including replicated logos, copied brand assets, and familiar website layouts that may evade traditional text-based detection methods.[1428] Amazon indicates that potential phishing websites identified by the system are subsequently reviewed through a combination of third-party verification and human assessment before takedown actions are initiated.[1429]

[1426] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

[1427] Amazon, 2025 Trustworthy Shopping Experience Report (2025), available at: https://trustworthyshopping.aboutamazon.com/2025-trustworthy-shopping-experience-report.

[1428] ibid.

[1429] ibid.

Designated service	Measure description
	Amazon reports that its AI and machine-learning systems analyse transaction patterns, customer interactions, seller activity, and other behavioural signals to identify anomalous activity and assess fraud risks throughout the seller lifecycle, and that machine-learning models are also used to analyse review activity using account linkages, sign-in activity, review histories, and other unusual behavioural patterns to detect and remove fake or incentivised reviews. The platform also indicates that these systems are supplemented by specialist fraud investigators.
Apple App Store	Apple App Store indicates that machine-learning models monitor user reviews to identify scams and support content moderation efforts.
Bing	Bing reports that it uses automated content detection systems to identify potentially non-compliant content and advertising, and that these systems combine machine learning models, heuristic analysis, and rules-based controls. Further, it indicates that Microsoft's advertising integrity systems are designed to identify evasive advertiser behaviour after approval.[1430] Reportedly, the system may automatically pause advertisements where indicators such as bot-net traffic, abnormal click clusters, or spoofed proxy locations are detected.[1431] Bing also indicates that Microsoft Video Authenticator analyses images and videos to estimate the likelihood of synthetic manipulation.[1432] Per the Report, content Credentials and cryptographic watermarking technologies are also used to support provenance verification of AI-generated images.
Booking.com	Booking.com reports that it uses AI models to identify potentially fraudulent or non-existent properties before they become available to travellers.
Google designated services (all)	Google reports that its automated systems analyse review activity to identify anomalous reviewing patterns, including unusual concentrations of ratings and suspicious reviewer, business, or network behaviour.
Google Play	Google Play reports that its Protect system analyses app behaviour and permissions to identify applications that may facilitate financial fraud, particularly when users attempt to install apps from external sources outside the official app store ecosystem.[1433]

[1430] Microsoft, Advertising Policies, available at: https://help.ads.microsoft.com/#apex/ads/en/60223/-1.

[1431] ibid.

[1432] Microsoft, New steps to combat disinformation and deepfakes with NewsGuard's Video Authenticator (2020), available at: https://blogs.microsoft.com/on-the-issues/2020/09/01/disinformation-deepfakes-newsguard-video-authenticator.

[1433] Google, Fraud and Scams Advisory (2025), available at: https://blog.google/innovation-and-ai/technology/safety-security/fraud-and-scams-advisory-november-2025/; Google, How We Kept Google Play and the Android App Ecosystem Safe in 2024 (2025), available at: https://blog.google/security/how-we-kept-google-play-android-app-ecosystem-safe-2024/.

Designated service	Measure description
Google Shopping	Google Shopping reports that it protects shoppers by removing fake reviews and utilising signals to proactively minimise abuse and spam, using automated vetting, store badges and other visual cues which help point out quality businesses.[1434]
LinkedIn	LinkedIn indicates that it uses machine-learning systems and anti-abuse models to detect fraudulent job postings and related abusive activity patterns.
Meta designated services	Meta describes using AI systems to analyse relationships between text, images, videos, URLs and account behaviour simultaneously. Accordingly, these systems are designed to identify "celeb-bait" scams involving unauthorised celebrity images, fake endorsements, impersonation schemes, and deceptive content intended to redirect users toward fraudulent websites. According to Meta, the technology allows a broader range of deceptive behaviours to be detected with greater precision than earlier rule-based systems.[1435] Additionally, Meta reports developing AI tools capable of reverse engineering AI-generated images in order to trace their origin. The detection software would look for signs of manipulation and help the human reviewer decide on the authenticity with an explainable AI report on these signs.[1436] Facebook Facebook reports that its machine-learning systems analyse user behaviour and account characteristics to identify impersonation, scam tactics, and other policy violations. Facebook additionally reports monitoring suspicious URLs at scale and testing AI systems designed to flag unusual friend requests, such as those originating from accounts with few mutual connections or geographic patterns inconsistent with normal user behaviour, to stop scams, such as romance scams.[1437] For Facebook Messenger, Meta reports implementing AI scam review systems that prompt users to share recent messages to analyse conversational characteristics associated with known scam patterns and

[1434] Google, Tackling scams and fraud together – Google white paper (2024), available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Tackling_scams_and_fraud_together.pdf.

[1435] TechBuzz, Meta deploys AI scam detection across all platforms (2026), available at: https://www.techbuzz.ai/articles/meta-deploys-ai-scam-detection-across-all-platforms; Meta, Meta launches new anti-scam tools, deploys AI technology to fight scammers and protect people (2026), available at: https://about.fb.com/news/2026/03/meta-launches-new-anti-scam-tools-deploys-ai-technology-to-fight-scammers-and-protect-people/; Meta, Fighting scammers: Protecting people with new technology and partnerships (2026), available at: https://about.fb.com/news/2026/03/fighting-scammers-protecting-people-with-new-technology-and-partnerships/.

[1436] ibid.

[1437] ibid.

Designated service	Measure description
	interactions with newly established contacts.[1438] Accordingly, if a potential scam is detected, the user receives a warning with different action options to take.[1439]
Pinterest	Pinterest indicates that its automated tools detect content identified as potentially violating the policies. Accordingly, machine-learning models assign scores to content, which are used by the automated tools to take appropriate enforcement actions. Pinterest states that when its automated tools detect violating content, the platform deactivates it or limits the distribution.
Pornhub	Pornhub reports the use of automated detection mechanisms as part of its content moderation framework; these include automated scanning tools that assess uploaded content before publication. The platform states that images and videos are scanned against hash databases of known child sexual abuse material (CSAM), with matching content prevented from being published. Pornhub also reports using additional detection tools to identify potentially underage performers in uploaded content, with the results of these automated checks provided to human moderators to support publication decisions. The platform further indicates that automated fingerprinting technologies are used to prevent previously identified illegal material from being re-uploaded.
Snapchat	Snapchat reports that it uses automated web-crawling technologies to analyse advertiser landing pages, as well as connected domains, product pages, sitemap entries, and conversion destinations. The platform holds that such systems enable the identification of fraudulent websites, misleading offers, and deceptive advertising destinations that may not be apparent during initial advertisement review. Specifically, Snapchat refers to its SnapchatAdsBot, which crawls the landing page URLs of ads that have been submitted to Snapchat as well as the domain for any landing page URL of ads that have been submitted to Snapchat, pages that fire conversion requests, and product pages listed in Sitemaps linked via robots.txt.[1440] For these additional URLs, SnapchatAdsBot reportedly uses web crawling protocols that attempt to adhere to standard robots.txt protocol.[1441]
Shein	Shein reports that it uses automated content moderation tools, such as an image search engine, to detect and remove problematic products, listings, accounts, reviews and other content. Additionally, Shein indicates that its scam detection systems monitor user activity on the Marketplace to detect patterns indicative of fraudulent behaviour, based on anomalies, and that user behaviour is analysed to identify deviations from normal patterns.

[1438] Meta, Fighting scammers: Protecting people with new technology and partnerships (2026), available at: https://about.fb.com/news/2026/03/fighting-scammers-protecting-people-with-new-technology-and-partnerships/.

[1439] ibid.

[1440] Snapchat, AdsBot Crawler, available at: https://businesshelp.snapchat.com/s/article/adsbot-crawler?language=en_US.

[1441] ibid.

Designated service	Measure description
Temu	Temu indicates that its automated systems detect non-compliant products using combined image, text, and seller-behaviour analysis to identify counterfeit goods, misleading listings, and scam patterns.
TikTok	TikTok states that its automated systems detect fraudulent and deceptive content, spam, coordinated inauthentic behaviour, fake engagement patterns, manipulated media, and synthetic content. The platform also indicates that these systems are also used to identify coordinated scam campaigns through behavioural and network-level signals.
Wikipedia	No specific information is provided by Wikipedia in its Report.
X	X reports using machine learning and heuristic models to detect platform manipulation, spam and abusive behaviour.
XNXX	XNXX indicates that it uses automated systems to analyse videos, images and text, including through technologies such as MD5 hashing for duplicate detection, Vercury for video and image fingerprinting, and AI-based tools such as Hive and Google SafetyNet API to identify potentially harmful content or assess risks related to prohibited material. XNXX also reports the use of keyword-based detection mechanisms, including blocklists and grey lists, to identify potentially problematic text content.
XVideos	XVideos reports that it uses automated tools and AI technologies to identify potentially illegal or policy-incompatible content across videos, images and text, enabling the platform to flag or remove problematic material more efficiently.
Zalando	Zalando indicates that it uses detection algorithms to detect and prevent harmful, misleading or inappropriate content and suspicious merchant behaviour stemming from product reviews and marketing activities.

Human review

Table 20 - Overview of human review measures as reported by the designated services[1442]

Designated services	Measure description
AliExpress	AliExpress describes that dedicated moderation teams manually review listings flagged by automated systems, assessing both text and images against platform rules. It also notes that human reviewers investigate suspected product mis-categorisation, conduct routine platform sweeps, perform user-like searches for infringing products, and review high-traffic content, and that dedicated Quality Assurance and inspection teams continuously monitor platform content and follow standard operating procedures when reviewing algorithmically flagged products.
Amazon Store	Amazon Store reports that specialist investigators review listings, sellers, reviews, and fraud signals identified through automated systems. Accordingly, its human investigators use proprietary fraud-detection tools to assess suspected fake reviews, counterfeit activity, policy violations, and scam operations. Amazon also notes that separate investigative teams conduct proactive searches of external social media platforms to identify review-manipulation schemes and organised abuse networks, while specialist fraud and abuse teams also evaluate the effectiveness of moderation systems and investigate coordinated scam operations.
Apple App Store	Apple App Store reports that every app submission and app update undergoes review by trained human reviewers who assess compliance with App Store policies before publication. Reportedly, human reviewers work alongside automated screening systems and conduct case-specific assessments where potential policy violations are identified.
Bing	Bing reports that human investigators review merchant listings, advertisements, and suspicious activity identified by automated systems. It also notes that dedicated investigation teams analyse evolving scam operations, including actors that rotate domains, URLs, phone numbers, and other identifiers to evade automated detection. Accordingly, human analysts use graph-analysis outputs to attribute related activities to broader scam networks and coordinate enforcement actions.
Booking.com	Booking.com reports that its dedicated cybersecurity and fraud-investigation teams review suspicious activity, investigate security incidents, and assess fraud risks identified through technical monitoring systems.
Google designated services	Google indicates that trained operators and analysts manually review ratings, reviews, and other content identified through automated moderation systems. Accordingly, human reviewers assess whether suspicious patterns identified by automated systems constitute policy violations and determine appropriate enforcement actions.
LinkedIn	LinkedIn reports that its human reviewers assess cases escalated by automated abuse-detection systems, particularly where account authenticity, fraudulent job postings, or coordinated account activity requires contextual evaluation, and that additional review may be conducted for accounts assigned intermediate abuse-risk scores.

[1442] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

Designated services	Measure description
Meta designated services	Meta describes that human reviewers assess content, accounts, advertisements, and behavioural patterns escalated by automated detection systems. Accordingly, specialist investigation teams conduct network-level investigations into coordinated scam operations, scam centres, impersonation campaigns, and organised fraud schemes. Meta also states that human investigators review outputs generated by AI-based scam-detection and synthetic-media detection systems before enforcement decisions are taken.
Pinterest	Pinterest indicates that human reviewers assess content escalated by automated classification systems, particularly where risk scores indicate potential policy violations requiring contextual evaluation. The platform also notes that review outcomes determine whether content is removed, restricted, or allowed to remain available.
Pornhub	Pornhub states that human moderation is used alongside automated detection systems to review flagged content and user reports before enforcement action. Pornhub indicates that disclosure remains high-level and does not include structured reporting on scale or allocation of human review.
Shein	Shein reports that content identified through automated review systems is escalated to human reviewers for verification and enforcement assessment before final action is taken.
Temu	Temu reports that human moderation teams review products, sellers, and listings escalated by automated detection systems, including suspected counterfeit products, prohibited goods, misleading listings, and repeat-offender cases. The platform also indicates that human review informs escalation decisions under Temu's graduated enforcement framework.
TikTok	TikTok reports that human moderators review content escalated by automated detection systems, assess potentially scam-related content, and conduct additional review of high-reach or high-impact content. Accordingly, escalated cases may be reviewed by specialist trust and safety teams before enforcement action is taken.
Wikipedia	Wikipedia reports that volunteer editors and administrators review suspected policy violations, investigate potentially deceptive activity, and determine whether content should be removed or accounts sanctioned.
X	X states that its human reviewers conduct manual reviews of content for potential rule violations, including through periodic sweeps and event-based monitoring, and that content identified by machine-learning and heuristic systems is escalated for review. X indicates that its moderators follow a structured "information-first" assessment process designed to improve consistency and reduce bias, and that review operations are conducted by multilingual teams providing 24-hour coverage.
XNXX	XNXX reports that human moderation is used in combination with automated systems to review flagged content and determine enforcement actions.
XVideos	XVideos reports that human moderators review content flagged by users and automated systems as part of enforcement decision-making.
Zalando	Zalando indicates that human moderation and compliance teams review content, reviews, listings, and seller activity escalated by automated detection systems, particularly where platform rules, consumer protection obligations, or marketplace integrity concerns require contextual assessment.

Removal and suspension mechanisms

Table 21 - Overview of removal and suspension mechanisms as reported by the designated services[1443]

Designated services	Measure Description
AliExpress	AliExpress reports that removal and restriction mechanisms are triggered following automated detection of fraud, counterfeit goods, or policy-violating behaviour. According to the platform, enforcement is based on combined signals from automated moderation systems, transaction monitoring, logistics anomaly detection, and seller behaviour analytics. AliExpress also indicates that fraudulent reviews identified through machine-learning systems (e.g., coordinated review manipulation, abnormal account linkages, suspicious sign-in behaviour) are removed, and that accounts linked to fraudulent activity are restricted, suspended, or removed. The platform indicates that listing-level enforcement includes removal of prohibited products, correction of miscategorised listings, and deactivation of seller privileges where repeated violations are detected.
Amazon Store	Amazon Store reports applying a multi-layered enforcement system combining automated detection, specialist investigator review, and trusted flagger mechanisms. Accordingly, listings identified as counterfeit, infringing, or fraudulent may be blocked at submission, escalated for manual verification, or removed following validation and seller accounts may be suspended or permanently removed in cases of repeated or severe violations. Amazon also describes its Project Zero initiative, which would allow verified brand owners to directly remove counterfeit listings (self-service enforcement mechanism functioning as an extended trusted flagger model). Amazon also states that enforcement extends across listings, reviews, sellers, and external impersonation domains identified through fraud intelligence systems.
Apple App Store	Apple App Store reports that enforcement operates at the submission and post-publication stages, and that all applications and updates undergo automated screening and human review before approval. The platform states that non-compliant applications may be rejected before publication, removed post-publication, or have developer accounts restricted or terminated in cases of repeated violations. It also describes an enforcement process that covers apps facilitating fraud, policy breaches, or misleading functionality.
Bing	Bing reports combining machine-learning models, heuristic systems, rules-based filtering, and manual review. Per Bing, advertisements may be rejected at submission stage, suspended post-approval, or permanently disabled following detection of policy violations or evasive advertiser behaviour. The service provider also reports that it applies post-approval integrity monitoring, including detection of bot-driven traffic, abnormal click patterns, and proxy-based manipulation, and that fraudulent advertiser accounts and associated campaigns may be suspended.

[1443] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

Designated services	Measure Description
Booking.com	Booking.com reports that it removes fraudulent, non-existent, or deceptive listings following detection through automated systems and risk monitoring tools. Accordingly, enforcement includes delisting properties, suspending host accounts, and restricting platform access where fraud or abuse is identified.
Google designated services	Google indicates applying content removal, advertiser suspension, and account-level enforcement where content violates policies or legal requirements across all its designated services. Accordingly, advertisements may be rejected at submission, removed post-publication, or escalated under a structured enforcement framework including a "three-strikes" policy for repeated violations. Google Ads Google indicates that policy-violating advertisements may be rejected before publication or removed after publication, while repeated policy violations may trigger escalating enforcement measures, including advertiser account suspension under Google's strike-based enforcement framework. Google Play Google indicates that on Google Play, apps identified as malicious or facilitating fraud may be removed or blocked via Google Play Protect, including apps installed outside the official store. Google Search Google indicates that on Google Search, enforcement focuses on removing or reducing the visibility of content that violates applicable policies, including through removal from search results where appropriate and other ranking or visibility-related interventions.
LinkedIn	LinkedIn reports that it uses automated abuse-detection systems and risk-scoring models, as follows: high-risk accounts may be automatically blocked or restricted, while medium-risk cases are escalated to additional verification processes and human review. Fraudulent job postings, impersonation accounts, and coordinated abuse networks may result in account removal or suspension.
Meta designated services	Facebook and Instagram report applying a multi-tier enforcement framework described as "remove, reduce, and inform".[1444] Accordingly, enforcement includes content removal, account suspension, advertiser restrictions, and network-level disruption of coordinated fraud operations. Meta indicates that scam-related accounts, pages, and advertisements may be removed following automated detection or human review escalation. Facebook and Instagram also report applying enforcement at network level, including coordinated inauthentic behaviour (CIB) takedowns, impersonation removal (including "celeb-bait" schemes), and advertiser bans. Accordingly, repeat offenders may be subject to escalating account-level restrictions and platform-wide disabling of advertising privileges.
Pinterest	Pinterest reports that it mainly relies on machine-learning risk scoring systems, as follows: content exceeding risk thresholds is automatically removed or deactivated, while lower-confidence cases may have distribution restricted (reduced visibility) or be escalated for human review. Moreover, accounts associated with repeated violations may face suspension or removal.
Pornhub	No specific information is provided by Pornhub in its Report.

[1444] Meta, Taking Action, available at: https://transparency.meta.com/enforcement/taking-action/.

Designated services	Measure Description
Snapchat	Snapchat indicates that removal combines automated ad review, post-submission monitoring, advertiser integrity investigations, and domain-level crawling systems. The platform indicates that ads may be rejected at submission or removed following detection of fraudulent landing pages or deceptive advertising infrastructure, and that advertiser accounts may be suspended where violations persist or where deceptive practices are detected across campaigns or domains.
Shein	Shein describes that content moderation is conducted through automated systems and human review escalation. The platform indicates that fraudulent listings, reviews, products, or accounts identified through monitoring systems are removed or restricted, and that its enforcement processes include takedown of non-compliant content and restriction of seller accounts, depending on severity and recurrence of violations.
Temu	Temu reports that its enforcement process is structured through a graduated three-tier system based on severity, intent, and recurrence. The measures reported by Temu include content or listing removal, progressive restrictions on seller activity, and permanent inclusion on a Trader Blocklist for repeated or severe violations, with enforcement described by the platform as applying to products, sellers, and platform listings.
TikTok	TikTok reports removing scam-related content, including deceptive investment schemes, fake earnings claims, and fraudulent offers, often before large-scale distribution. TikTok indicates that enforcement escalates from warnings to account-level penalties, including temporary suspensions and permanent account termination for repeated or severe violations. Accordingly, automated systems support early detection of spam, coordinated inauthentic behaviour, and manipulated content, followed by review and enforcement actions.
Wikipedia	Wikipedia indicates that enforcement is conducted through volunteer moderation structures, and that the content that violates platform policies is removed, edited, or reverted by editors and administrators. The platform also reports that accounts engaging in persistent abuse may be blocked or banned, and that its enforcement process is decentralised and community-driven rather than automated.
X	X reports that its enforcement includes content removal, visibility filtering, and account-level restrictions, with machine-learning and heuristic systems used to identify spam, manipulation, and abusive behaviour. X also indicates that accounts may be suspended or permanently removed depending on severity and recurrence.
XNXX	XNXX indicates that content identified as illegal or policy-violating through automated detection systems is removed, and that its enforcement processes are primarily automated.
XVideos	XVideos reports that its machine-learning systems are used to detect illegal content, and that its enforcement process includes removal of such identified content.
Zalando	Zalando indicates that enforcement includes removal of misleading content, suspension of merchant accounts, and restriction of listings. The platform reports that its risk-based detection systems identify suspicious merchant behaviour across product listings, reviews, and marketing activity, and that repeated violations may result in account termination or exclusion from platform participation.

Detection of coordinated scam networks

Table 22 - Overview of detection measures of coordinated scam networks as reported by the designated services[1445]

Designated service	Measure description
AliExpress	AliExpress describes tracking systems and databases containing information relating to fraudulent account holders, enabling the identification of recidivist behaviour, account takeovers, re-entry attempts by banned sellers, and coordinated manipulation of platform systems.
Amazon Store	Amazon Store reports using traditional fraud-detection systems, which assess suspicious signals individually, and newer systems based on knowledge graphs and deep graph neural networks. Accordingly, these systems can uncover relationships between accounts, transactions, reviews, sellers, and behavioural indicators that would remain invisible if each signal were assessed independently. Amazon indicates that these processes enable it to identify fake review rings, counterfeit networks, refund scam schemes, and broader scam operations by uncovering hidden relationships between actors and detecting patterns of coordinated behaviour.[1446]
Apple App Store	No specific information is provided by Apple App Store in its Report.
Bing	Bing reports that by combining web-scale graph analytics with human analysis, it can trace fraudulent infrastructure back to known threat actors and disrupt entire networks of interconnected scam storefronts rather than addressing individual violations in isolation.[1447]
Booking.com	No specific information is provided by Booking.com in its Report.
Google designated services	Google reports using LLMs and behavioural detection systems to identify interconnected networks of deceptive websites, coordinated spam operations, and ranking-manipulation schemes that may appear legitimate when examined individually.[1448]
LinkedIn	LinkedIn reports focusing on coordinated account creation, describing machine-learning registration scoring systems designed to identify groups of accounts exhibiting similar behavioural characteristics or appearing to be controlled by the same actor. LinkedIn indicates that

[1445] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

[1446] Amazon, 2025 Trustworthy Shopping Experience Report (2025), available at: https://trustworthyshopping.aboutamazon.com/2025-trustworthy-shopping-experience-report.

[1447] Microsoft, Advertising Policies (n.d.), available at: https://help.ads.microsoft.com/#apex/ads/en/60223/-1; David Urosevic, Roberto Rodriguez, Kristina Lerman, and Gianluca Stringhini, Countering Technical Support Scams (2019), available at: https://www.microsoft.com/en-us/research/wp-content/uploads/2018/12/CounterTechSupportScams.pdf.

[1448] Google, Fighting Search Scams with AI (2024), available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Search-Scam-Report-0508.pdf.

Designated service	Measure description
	it assigns each account registration attempt an abuse-risk score, blocking high-risk accounts and subjecting medium-risk accounts to additional verification requirements.[1449] LinkedIn reports that these systems have prevented large-scale fake account creation campaigns, including one instance in which 5 million fake accounts were blocked within a single day.[1450]
Meta designated services	Facebook and Instagram report identifying and disrupting networks of fraudulent accounts, coordinated inauthentic behaviour, and organised scam operations through behavioural analysis, account-linkage signals, and cross-platform investigations. They also report disabling millions of accounts associated with scam centres and undertaking targeted enforcement against organised criminal operations, including 1,620 assets linked to networks involved in sextortion and other coordinated fraud schemes.[1451] Instagram According to Meta, more than 7 million Instagram accounts linked to organised scam centres operating across multiple countries have been detected and disrupted since 2024.[1452]
Pinterest	Pinterest reports using automated systems to identify patterns of coordinated spam and linked policy-violating activity across accounts, enabling enforcement against broader abuse networks rather than isolated content items.
Pornhub	No specific information is provided by Pornhub in its Report.
Snapchat	Snapchat reports using automated integrity and enforcement systems to identify coordinated advertising abuse, including networks of related advertiser accounts, repeated policy-circumvention attempts, and other patterns indicating linked actors operating across multiple accounts or campaigns. The platform indicates that these systems support the detection and disruption of broader abusive advertising operations rather than isolated policy violations.
Shein	No specific information is provided by Shein in its Report.
Temu	No specific information is provided by Temu in its Report.
TikTok	TikTok reports detecting coordinated deceptive activity through behavioural analysis and integrity systems designed to identify networks of fake engagement, coordinated spam activity, and groups of accounts acting in concert to manipulate platform systems.
Wikipedia	No specific information is provided by Wikipedia in its Report.

[1449] LinkedIn Engineering, Automated Fake Account Detection at LinkedIn (2022), available at: https://www.linkedin.com/blog/engineering/trust-and-safety/automated-fake-account-detection-at-linkedin.

[1450] ibid.

[1451] TechBuzz, Meta deploys AI scam detection across all platforms (2026), available at: https://www.techbuzz.ai/articles/meta-deploys-ai-scam-detection-across-all-platforms.

[1452] ibid.

Designated service	Measure description
X	X indicates that machine-learning and heuristic detection systems are used to identify coordinated activity, platform manipulation, spam campaigns, and groups of accounts exhibiting linked behavioural patterns indicative of coordinated operations.
XNXX	No specific information is provided by XNXX in its Report.
XVideos	No specific information is provided by XVideos in its Report.
Zalando	No specific information is provided by Zalando in its Report.

Recommender system protection measures

Table 23 - Overview of recommender systems as reported by the designated services[1453]

Designated service	Measure description
AliExpress	AliExpress indicates that its recommendation pool is linked to Chief Risk Office controls, so that products flagged through compliance and risk-management processes are automatically excluded from recommendation eligibility. The platform also reports that products with consistently negative buyer feedback are removed from recommendation pools, reducing the visibility of potentially problematic listings.
Amazon Store	Amazon Store reports that its search and recommendation systems include customer-trust safeguards. The platform states that where customer queries indicate an intent to locate infringing products, autocomplete suggestions may be suppressed and no search results returned. Amazon further states that products presenting safety or customer-trust risks may be excluded from recommendation surfaces.
Apple App Store	No specific information is provided by Apple App Store in its Report.
Bing	No specific information is provided by Bing in its Report.
Booking.com	No specific information is provided by Booking.com in its Report.
Google designated services	Google Search Google identifies ranking quality and anti-manipulation systems as part of its anti-scam strategy. It states that its ranking systems prioritise signals associated with expertise, authoritativeness, and trustworthiness in order to surface “people-first” rather than “search-engine-first” content.[1454] Google also indicates that since 2022, it has introduced measures specifically targeting forms of "scaled content abuse".[1455] Google additionally reports enforcement against "site reputation abuse", whereby third parties exploit trusted domains to host misleading content that benefits from the reputation and ranking authority of the host website, as well as "expired domain abuse", where previously reputable domains are repurposed to artificially boost the visibility of deceptive material.[1456]

[1453] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

[1454] Google, Creating Helpful, Reliable, People-First Content, available at: https://developers.google.com/search/docs/fundamentals/creating-helpful-content.

[1455] ibid.

[1456] Google, How Search Works: Ranking Results, available at: https://www.google.com/intl/en_us/search/howsearchworks/how-search-works/ranking-results/; Google, New Spam Policies to Tackle Low-Quality Content in Search (2024), available at: https://blog.google/products-and-platforms/products/search/google-search-update-march-2024/.

Designated service	Measure description
	Google Maps Google reports that classifiers are used on Google Maps to detect inauthentic engagement practices intended to manipulate visibility and rankings within mapping and review systems.
LinkedIn	No specific information is provided by LinkedIn in its Report.
Meta designated services	Facebook Facebook reports that it uses ranking interventions, demotion measures, recommendation eligibility restrictions, and integrity-based ranking signals. Instagram Instagram reports that its recommendation systems incorporate integrity signals and recommendation eligibility criteria. It further describes that certain categories of borderline, misleading, or policy-adjacent content may remain available but become ineligible for recommendation surfaces such as Explore or suggested content feeds.
Pinterest	Pinterest indicates that its recommendation-system integrity measures reduce the visibility of spam, misleading content, and low-quality recommendations through ranking-quality signals and recommendation eligibility criteria.
Pornhub	No specific information is provided by Pornhub in its Report.
Snapchat	Snapchat indicates that it distinguishes between content moderation decisions and recommendation eligibility decisions. The platform reports that certain forms of "engagement bait" are categorised as "Not Eligible for Recommendation", including misleading or sensationalised content designed primarily to manipulate views, interactions, rewatches, or shares. Examples provided by Snapchat include deceptive "wait for it" captions, artificial engagement incentives, misleading platform challenges, and other techniques intended to exploit recommendation systems through behavioural manipulation rather than genuine user interest.
Shein	No specific information is provided by Shein in its Report.
Temu	No specific information is provided by Temu in its Report.
TikTok	TikTok reports interventions aimed at reducing scam-related amplification dynamics, including additional moderation of highly viral content, manual review of content reaching specific popularity thresholds, and machine-learning-based “dispersion techniques” designed to prevent repeated recommendation of similar potentially harmful content. TikTok states that it provides user controls to adjust recommendation outputs and reduce exposure to unwanted content categories.
Wikipedia	No specific information is provided by Wikipedia in its Report.
X	X reports that visibility filtering, ranking interventions, reduced amplification of policy-violating content, and integrity-based ranking signals are used.

Designated service	Measure description
XNXX	No specific information is provided by XNXX in its Report.
XVideos	No specific information is provided by XVideos in its Report.
Zalando	Zalando indicates that its product recommendation and ranking systems incorporate trust and quality signals intended to prioritise reliable merchants and reduce visibility of problematic listings.

Reporting tools

Table 24 - Overview of reporting tools as reported by the designated services[1457]

Designated services	Measure Description
AliExpress	AliExpress reports operating a notice-and-action reporting infrastructure as part of its post-listing monitoring framework. Accordingly, the mechanism is available to three distinct user categories – buyers, sellers, and non-registered users – and can be accessed via a clearly labelled, dedicated reporting button. AliExpress states that users can flag content as potentially illegal or as incompatible with the platform's Terms and Conditions, and that an integrated appeal mechanism allows users to challenge content moderation decisions through a dedicated link included in the decision notification. The platform additionally reports operating a separate intellectual property protection reporting pathway for rights holders. AliExpress expresses its commitment to providing reporters with feedback on appeals in due course, including information on redress possibilities and on whether automated means were used to process the notice. The platform claims that its reporting infrastructure sits within a broader post-listing monitoring system that pairs user-initiated reports with the platform's own proactive content surveillance. No reporting category specifically labelled for financial scams is described in the platform's documentation; scam-related reports – such as listings for fraudulent goods or deceptive offers – are submitted through the general illegal-content channel. The 2025 Independent Audit of AliExpress concluded that the platform generally complied with its obligations under Article 16 DSA, while identifying slight shortcomings in relation to certain requirements.[1458] For example, the Independent Audit held that notice-and-action mechanisms were not consistently easy for users to access.[1459]
Amazon Store	Amazon Store indicates that its primary notice-and-action mechanism for EU users is the "Report an Issue with this product" feature, which is available on each individual product page. To submit a report, users must be logged in to their Amazon account; Amazon has stated that this authentication requirement is designed to protect against abuse and misuse of the mechanism. The platform indicates that the mechanism allows any individual or entity – including Trusted Flaggers – to submit notices concerning illegal products or content, with Trusted Flaggers' submissions given priority processing.

[1457] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

[1458] FTI Consulting, Independent Audit of AliExpress – Article 37 of Regulation (EU) 2022/2065 (Digital Services Act), available at: https://www.dropbox.com/scl/fi/8mn8wigchllrxpp4kypkz/2025-Audit-Report.pdf?rlkey=lntmlgoo5evtvxo6qa3s6xeuh&st=p1l4ehg7&e=1&dl=0.

[1459] ibid.

Designated services	Measure Description
	Amazon also reports that it maintains a "Report Abuse" function accessible at the level of individual customer reviews, through which users can flag reviews they consider abusive or manipulative. For reports relating to scam communications received outside the platform – such as phishing emails, fraudulent text messages, or spoofed correspondence – Amazon indicates that it maintains a dedicated email address (reportascam@amazon.com) to which users can forward suspicious communications as attachments. The platform also notes that sellers can report policy violations, counterfeit goods, and fraudulent conduct through the "Report Abuse" tool in Amazon Seller Central, selecting from a menu of violation types. No dedicated scam or fraud reporting category is described as a distinct option within the product-page notice-and-action form. The 2025 Independent Audit of Amazon EU S.à r.l. provided mixed conclusions on the platform's implementation of Article 16 notice and action mechanisms.[1460] The Independent Audit's views were positive for Article 16(2), positive with comments for Article 16(1), negative for Article 16(5), and for Article 16(6), negative for the first half of the evaluation period (July-December 2024) but positive with comments for the second half (January-June 2025) after concerns were addressed.[1461]
Apple App Store	Apple App Store describes two parallel reporting pathways for the App Store. The first is the "Report a Problem" tool, available both within the App Store application and at the web portal reportaproblem.apple.com. Apple reports that through this tool, users can select from a set of predefined categories, including – since iOS 15 – a dedicated "Report a scam or fraud" option, as well as options to report offensive, abusive, or illegal content, or to request a refund. Apple notes that the scam or fraud option was added in 2021 in response to criticism that the App Store lacked a direct pathway for reporting fraudulent applications. The second pathway described by Apple is a dedicated DSA notice-and-action mechanism accessible at ContentReports.apple.com or through the "Report a Problem" tool for users with an EU IP address. Apple indicates that this mechanism is open to any individual or entity, including Trusted Flaggers and EU Member State authorities submitting orders to act against illegal content under Article 9 DSA. According to the Report, the App Store moderates three categories of content through these mechanisms: live apps, App Store advertisements, and user ratings and reviews; reports submitted through the "Report a Problem" mechanism are routed to human moderators for review. Apple also indicates that the web portal at reportaproblem.apple.com covers free apps that do not offer in-app purchases, extending the scope of reportable content beyond paid downloads.

[1460] KPMG, DSA Assurance Report – Independent practitioner's assurance report concerning Regulation (EU) 2022/2065, the Digital Services Act (DSA), available at: https://www.dropbox.com/scl/fi/4weflzsc8jqs2zhr0xyq1/eu-dsa-audit-report-amazon-2025.pdf?rlkey=p2xi6la8ifh2npf6ofi9rjosi&st=tlzb82dk&e=1&dl=0.

[1461] ibid.

Designated services	Measure Description
	The 2025 Independent Audit of the App Store provided a positive conclusion on the platform's implementation of notice and action mechanisms under Article 16 DSA.[1462]
Bing	On the user-facing side, Bing states that it provides avenues through which users can report ad suggestions they consider inappropriate, including those that appear to constitute phishing, financial fraud, or other scam-related content. Microsoft also reports maintaining a dedicated ad quality escalation form through which users who encounter a bad or suspicious advertisement can submit a report for review by Microsoft's policy and review specialists. The 2025 Independent Audit of Bing did not assess the platform's implementation of notice and action mechanisms under Article 16 of the DSA, as Bing maintains that Article 16 does not apply to its services.[1463]
Booking.com	Booking.com indicates that its reporting infrastructure combines automated detection with user-facing reporting channels. Accordingly, on the user-facing side, travellers can report content – including potentially fraudulent property listings, misleading accommodation descriptions, or suspicious in-platform communications – through general reporting avenues available on the platform. For partner properties, Booking.com describes that it provides a mechanism within its partner Extranet through which hosts can report suspected fraudulent bookings. To do so, a host selects the relevant reservation and reports it under the "Other" subtopic, which covers fake or fraudulent reservations. The platform indicates that for security incidents more broadly, partners can use security reporting tools within the Extranet. Booking.com reports that it maintains dedicated teams that monitor for fraudulent bookings using continuously updated detection models. No scam-specific reporting category for consumer-facing users is described in the platform's DSA documentation. Scam-related content falls within the platform's general user reporting avenues covering content that violates platform guidelines. The 2025 Independent Audit of Booking.com provided positive conclusions on the platform's implementation of notice and action mechanisms under Article 16 of the DSA.[1464]
Google designated services	Google reports operating a multi-surface reporting infrastructure spanning its various products and services. Accordingly, a centralised "Report Content on Google" portal provides two distinct reporting paths: a legal pathway for content that is illegal under EU or national law – covering, for example, content violating anti-fraud or consumer protection legislation – and a non-legal policy pathway for content that violates Google's own content policies, such as spam, phishing, or scam material. Google notes that users must specify the Google

[1462] EY, Independent Audit on the App Store, available at: https://www.dropbox.com/scl/fi/htdwuqum9fljh7mw7fjkn/20251119_app-store_reasonable-assurance-report_non-confidential.pdf?rlkey=khz719r2fc8zn3rxaesfmqp4y&st=1xb8hi68&e=1&dl=0.

[1463] Deloitte, Microsoft Bing's Digital Services Act (DSA) Report, available at: https://www.dropbox.com/scl/fi/p7t7crqw6w54yu4qp98g2/August-2025-Microsoft-Bing-Audit-Report-EU-Digital-Services-Act.pdf?rlkey=bki161lb2jn5skzdarjrxgl6x&st=7i1q1plg&e=1&dl=0.

[1464] Deloitte, Booking.com B.V. Digital Services Act (DSA) Assurance Report, available at: https://www.dropbox.com/scl/fi/pct8bi29kykqq1tda58ct/2025-Audit-report.pdf?rlkey=t3mjd9dqmuer2rx4em6fyswwk&st=b7ohtnyo&e=1&dl=0.

Designated services	Measure Description
	product on which the content appears and the URL of the specific content being reported and are asked to provide a detailed explanation of the violation. Confirmation of receipt is provided by email. At the product level, Google indicates that it maintains separate in-product reporting tools. For Google Search, the platform describes a dedicated reporting form which allows users to report spam, phishing, or malware appearing in search results. Reportedly, Google uses these reports to improve its spam detection systems. For Google Ads and Shopping, a reporting tool allows users to flag individual ads or product listings, with categories including "scam/phishing, offensive, or dangerous content" and "legal violation." Google mentions that individual Google products such as Google Maps and Google Docs carry their own in-product abuse reporting flows. Google also states that user reports complement, rather than replace, Google's own proactive review processes, which include automated and manual moderation. The 2025 Independent Audit Reports of Google Maps, Google Play, and Google Shopping provided overall positive conclusions on the platforms' implementation of notice and action mechanisms under Article 16 of the DSA.[1465] The Independent Audit had comments on Google Play's implementation of Article 16 (1).[1466] The Independent Audit also considered that Google Shopping's implementation of Article 16 (2) was not in line with the requirements of the Regulation.[1467] The 2025 Independent Audit of Google Search did not assess the platform's implementation of notice and action mechanisms under Article 16 of the DSA, as Google Search maintains that Article 16 does not apply to its services.[1468]
LinkedIn	LinkedIn indicates operating a two-tier reporting structure. At the level of individual job postings, the platform describes that members can initiate a report through a "More" icon on the job detail page, which opens a dropdown including the option "Report this job." The subsequent reporting prompt offers a set of predefined categories, including "I think it's a scam, phishing or malware" – covering listings

[1465] EY, Independent Audit on Google Maps – Digital Services Act, available at: https://www.dropbox.com/scl/fi/iuyiw6po4ws12ikpaxy4f/2025-Audit-Report.pdf?rlkey=9lyr64ehlj2mrly2nomthc2ah&st=aqsg0ucn&e=1&dl=0; EY, Independent Audit on Google Play – Digital Services Act, available at: https://www.dropbox.com/scl/fi/81133n2f15wdsbmu8gx7n/2025-Audit-report.pdf?rlkey=7n715t6euz6myjwdq0yj4256o&st=18p4fs82&e=1&dl=0; EY, Independent Audit on Google Shopping – Digital Services Act, available at: https://www.dropbox.com/scl/fi/ti6dfeps05kwr5207h69m/2025-Audit-report.pdf?rlkey=7vfrm35jqjsle8pxgsmppy493&st=vylqyh0o&e=1&dl=0.

[1466] EY, Independent Audit on Google Play – Digital Services Act, available at: https://www.dropbox.com/scl/fi/81133n2f15wdsbmu8gx7n/2025-Audit-report.pdf?rlkey=7n715t6euz6myjwdq0yj4256o&st=18p4fs82&e=1&dl=0

[1467] EY, Independent Audit on Google Shopping – Digital Services Act, available at: https://www.dropbox.com/scl/fi/ti6dfeps05kwr5207h69m/2025-Audit-report.pdf?rlkey=7vfrm35jqjsle8pxgsmppy493&st=vylqyh0o&e=1&dl=0.

[1468] EY, Independent Audit on Google Search – Digital Services Act, available at: https://www.dropbox.com/scl/fi/o6z386lexmp3leeqtj0v4/2025-Audit-report.pdf?rlkey=pve1re0x1sisvdt34wdcm043z&st=ff73c5pm&e=1&dl=0.

Designated services	Measure Description
	that solicit personal information, request payment, post suspicious requirements, or otherwise exhibit hallmarks of recruitment fraud – as well as categories for discriminatory content and spam. LinkedIn states that reporters are not identified to the account being reported. For other content types across the platform – including profiles, messages, posts, and connection requests – LinkedIn indicates that it provides a broader reporting mechanism accessible through contextual menus, with a "Why are you reporting this?" prompt offering applicable categories including phishing, scams, spam, and malware. For messages specifically, users select the message, access a "More" menu, and choose "Report this conversation," followed by a reason from the same categorised prompt. LinkedIn reports that it may notify reporters of outcomes by email in some cases, and can take actions including warnings, content removal, or account suspension for confirmed violations. The 2025 Independent Audit of LinkedIn provided positive conclusions on the platform's implementation of notice and action mechanisms under Article 16 of the DSA.[1469] The Independent Audit also noted that initial processes, which, in the opinion of the auditors, were not in line with the Regulation, were subsequently remediated through an updated process implemented on December 19, 2024.[1470]
Meta designated services	Meta indicates that it operates reporting mechanisms across both Facebook and Instagram that share a common underlying architecture, while reflecting the distinct content surfaces and use contexts of each platform. On Facebook, Meta describes that a reporting option is integrated into nearly every piece of content on the platform. Users can access a contextual menu on posts, profiles, ads, Marketplace listings, comments, and other content surfaces to initiate a report. For organic content, the reporting flow includes a dedicated “Scam or fraud” category alongside other options such as false information and nudity. For advertisements, users can select “Report ad,” followed by “Misleading or scam ad,” and then “Send a detailed scam report,” which routes the report to a dedicated internal operations team. For Marketplace listings, users can report listings as fraudulent or as involving scam sellers. For profiles and pages, impersonation and fake account reporting options are available, covering pages pretending to be another business or organisation. Facebook’s community standards explicitly prohibit content designed to defraud users, covering a range of scam types including loan fraud, investment fraud, and payment scams. On Instagram, Meta describes that reporting tools are available for posts, stories, profiles, ads, and other content surfaces through contextual menus, with users selecting from a categorised list of violation types. Meta states that scam-related content is addressed within the platform’s “Deceptive and Misleading” content framework – a risk category covering behaviour and content designed to deceive, mislead, or defraud users for personal gain – rather than as a standalone reporting category. The complaints and appeals mechanisms on Instagram are described by Meta as longstanding, predating DSA-specific compliance obligations, and are reportedly made available both to users who submit a report and to users whose content has been subject to a moderation action.

[1469] Deloitte, LinkedIn’s Digital Services Act (DSA) and Code of Conduct on Countering Illegal Hate Speech Online (Code of Conduct) Report, available at: https://www.dropbox.com/scl/fi/nget5qj8vi7d3k778ybus/2025-Audit-Report.pdf?rlkey=ojbtgwz9ox9mbjolfbfp84ln1&st=0xe6y6tn&e=1&dl=0.

[1470] ibid.

Designated services	Measure Description
	Meta indicates that both its platforms process Article 16 DSA notices through manual review; a separate DSA illegal content reporting form is available for EU users to report content as illegal under EU or national law, distinct from the in-product reporting flows described above. Corresponding appeal forms allow users to contest moderation decisions on each platform. The 2025 Independent Audits on Facebook and Instagram respectively provided a positive conclusion on the platforms' implementation of notice mechanisms under Article 16 of the DSA.[1471]
Pinterest	Pinterest describes that its reporting mechanism is accessible through individual Pins and user profiles via a reporting button or contextual menu, and that users who wish to report a Pin can access a report option directly from the Pin surface. Accordingly, submitted reports are directed to a Content Reporting Form, which is reviewed manually by Pinterest's moderation teams. Pinterest does not describe a dedicated scam or fraud reporting category in its public documentation; user reports are processed against Pinterest's Community Guidelines and applicable law, with content deactivated globally or restricted to specific territories depending on whether it violates platform policies or only local law. The platform additionally handles government removal orders from EU Member States. The platform states that if a user frequently submits manifestly unfounded reports, Pinterest may, following a warning, suspend that user's ability to use the reporting system for a reasonable period. The 2025 Independent Audit of Pinterest provided positive conclusions on the platform's implementation of Article 16 notice and action mechanisms.[1472]
Pornhub	Pornhub notes that its primary user-facing reporting mechanism is a Content Removal Request (CRR) form, which is linked persistently at the bottom of every page on the platform. Pornhub indicates that the permanent, platform-wide placement of the link means that users can access the reporting form from any page without navigating to a separate help centre or support portal. Accordingly, the CRR is a general-purpose content removal tool; it does not present a categorised list of violation types, meaning users would employ the same form to report scam-related content – such as subscription fraud or financial deception linked to content access – as any other type of violating material. No dedicated scam or fraud reporting pathway is described in the platform's documentation.

[1471] EY, Independent Audit on Facebook, available at: https://www.dropbox.com/scl/fi/fbx16f0ieakgkersk2ctv/2025-Audit-Report.pdf?rlkey=zthd9c02o7gsoozctzyae2461&st=j02t2t0f&e=1&dl=0; EY, Independent Audit on Instagram, available at: https://www.dropbox.com/scl/fi/v3n2nxj7mg0m0gr71ljac/2025-Audit-Report.pdf?rlkey=lko1tvj4j1xmx6bwkzag5d318&st=wi6n41h4&e=1&dl=0.

[1472] EY, Independent Audit on Pinterest, available at: https://www.dropbox.com/scl/fi/kr9mkl9949jwkk53hcop0/Independent-Audit-of-Pinterest-DSA-Redacted-11102025.pdf?rlkey=h4u7k1kusb42beb5k76arhewz&st=l4rz1h4i&e=1&dl=0.

Designated services	Measure Description
	The 2025 Independent Audit of Pornhub provided positive conclusions on the platform's implementation of notice and action mechanisms requirements under Article 16 of the DSA.[1473]
Snapchat	Snapchat reports providing parallel reporting channels. The in-app reporting system is available to registered users: from within a Snap, Story, profile, or message, users can access a reporting option and select from a set of predefined categories. One of the categories is 'Illegal Content', within the meaning of the DSA. Another category is "Fraud and Spam", which is defined by Snapchat's terms and conditions (Snapchat Community Guidelines). Web-based reporting forms are accessible to any person, including non-users of the platform. Through one form, they may report Illegal Content.[1474] Through another, they may report content that goes against Snapchat's Community Guidelines.[1475] According to Snapchat, its safety teams review reports submitted through all channels and take action on content and accounts that violate community guidelines or terms of service. The identity of the reporting user is not disclosed to the reported account. Snapchat notes that for content that appears illegal or dangerous, users should also contact local law enforcement directly. The 2025 Independent Audit of Snapchat provided a positive opinion on the platform's compliance with Article 16 DSA requirements.[1476]
Shein	Shein describes that its notice-and-action mechanism is integrated at the individual content level: each product listing and each user review on the platform contains a reporting button enabling users to flag that content. Shein indicates that the button is embedded directly on the product or review page, so users can initiate a report without leaving the content in question, and that the mechanism covers any content that violates applicable law or Shein's terms and conditions. Shein indicates that it additionally operates a dedicated intellectual property reporting portal through which rights holders can submit IP infringement notices, including the upload of supporting documentation such as proof of ownership. Shein reports that its seller portal provides guidance on compliance requirements, and that sellers are required to confirm at the point of product upload that their listing does not constitute intellectual property infringement and meets applicable environmental standards. Shein

[1473] FTI Consulting, Independent Audit – Article 37 of Regulation (EU) 2022/2065 (Digital services Act), available at: https://www.dropbox.com/scl/fi/s1wvtx9ixpzcwemp7fsbs/Audit_Report_for_Pornhub_April_2025_1753199885.pdf?rlkey=75uu62kdzgvl9im25zlw9hqmr&st=czfkfyl1&e=1&dl=0.

[1474] Snapchat Support, Report Illegal Content, avaialble at: https://businesshelp.snapchat.com/s/report-illegal-content?language=en_GB.

[1475] Snapchat Support, Report Account or Content, available at: https://help.snapchat.com/hc/en-us/requests/new?co=true&tf_23701027754644=cf_report_violation_false_info_deceptive_practices_fraud_scams&ticket_form_id=17471023300884.

[1476] EY, Independent Audit on Snapchat, available at: https://www.dropbox.com/scl/fi/i93vef6fc38fhc2kgtakf/DSA_and_Hate_Speech_Code_of_Conduct_Reporting_Package_-_Snapchat_2025_Redacted.pdf?rlkey=p8f5kene5k74yulyicyoivkxz&st=cbi3cjho&e=2&dl=0.

Designated services	Measure Description
	indicates that reviews flagged as engaging in fraudulent activity may be temporarily or permanently withheld from publication. No dedicated scam or fraud reporting category is described; the general listing-level reporting button constitutes the mechanism through which potentially fraudulent product content would be reported. The 2025 Independent Audit of SHEIN provided a positive conclusion on the platform's implementation of mechanisms under Article 16 of the DSA.[1477]
Temu	According to Temu, its reporting function allows three categories of stakeholders – platform users, rights holders, and other relevant stakeholders – to flag potentially non-compliant products or reviews. Temu claims that this breadth of access extends the reporting mechanism beyond the consumer-facing user base to include IP rights holders and third parties with a legitimate interest in content on the platform. Temu indicates that all submitted reports are assigned to human moderators for review. The platform does not route user-submitted notices through automated-only processing. Temu also states that the moderation process covers both product listings and user reviews. For reviews, Temu reports employing automated scanning tools to detect inappropriate terms or phrases – covering, for example, private information, inappropriate language, and promotion of illegal activities – alongside the human review of user-submitted reports. For product listings, Temu indicates that automated tools scan for prohibited or non-compliant products and flag suspicious images for human review. No dedicated scam reporting category is described; the general reporting function covers non-compliant products and reviews, within which scam-related content would fall. The 2025 Independent Audit of Temu provided a positive conclusion on the platform's implementation of notice and action mechanisms under Article 16 of the DSA.[1478]
TikTok	TikTok indicates that it provides in-app reporting tools through which users can flag individual videos, accounts, comments, and live streams, and that reporting is initiated from a contextual menu on the relevant content, from which users can select a category of violation types. TikTok reports that in August 2023 it introduced an additional reporting mechanism specifically for illegal content under EU law, creating a distinct Article 16 pathway alongside the standard in-app reporting flow.

[1477] Deloitte, SHEIN – DSA Assurance Report, available at: https://www.dropbox.com/scl/fi/vaxfl4vttxcg8wj78feb4/2025-Audit-Report.pdf?rlkey=vc6iilli3101zyolwrv5y0w1f&st=qmfkmndl&e=1&dl=0.

[1478] EY, Independent Audit on TEMU, available at: https://www.dropbox.com/scl/fi/buv4tarf7mkf11vq5ec5n/DSA-Audit-Report-2025.pdf?rlkey=qtogc37szpbj32eredokjwujx&st=6gl4n32w&e=1&dl=0.

Designated services	Measure Description
	The 2025 Independent Audit of TikTok generally provided a positive conclusion on the platform's implementation of notice and action mechanisms under Article 16 of the DSA.[1479] The Independent Audit had comments on the implementation of Article 16(1) mechanisms for notifying illegal content.[1480] The Independent Audit reached a negative conclusion on Article 16(6) regarding the processing of notices and decision-making in a timely, diligent, non-arbitrary, and objective manner.[1481]
Wikipedia	Wikipedia does not describe dedicated reporting mechanisms for scam or fraudulent content in its DSA risk assessment and does not identify financial scams as a distinct risk category. The platform's risk assessment focuses on content-related risks specific to its encyclopaedic character – including disinformation, harassment, harmful content, illegal content, child rights, and algorithmic risks – and describes that its reporting mechanisms are tailored to those categories. No scam-specific or fraud-specific reporting pathway is described in the platform's public documentation. The 2025 Independent Audit of Wikipedia provided a positive with comments conclusion on the platform's implementation of notice and action mechanisms under Article 16 DSA.[1482]
X	X states that it has implemented two DSA-specific reporting tools for EU users: a dedicated illegal content reporting form, available at help.x.com/en/forms/dsa/report, and a separate appeal form through which users can contest content moderation decisions. The illegal content reporting form is framed by X as a general-purpose tool for reporting content that is illegal under EU or national law. No specific scam or fraud reporting category is designated within the DSA form; financial scam content would be reported as illegal content without a dedicated label. Separately, according to X's standard in-product reporting flow – accessible through a three-dot menu on individual posts, profiles, and advertisements – users can flag content for a range of reasons including spam, misleading information, and abusive content. X states that it has updated the statements of reasons provided to users whose content is the subject of a moderation decision.

[1479] KPMG, DSA Assurance Report, available at: https://www.dropbox.com/scl/fi/nldbvg99c59xrfmvja8qm/DSAAssuranceReport-TikTokTechnologyLimited-2025.pdf?rlkey=or3n1vnu5ocfub7oi3lejrf88&st=qgo9y1gj&e=1&dl=0.

[1480] ibid.

[1481] ibid.

[1482] Holistic AI, Independent Audit on Wikipedia, available at: https://www.dropbox.com/scl/fo/mygrijkpirx0h48mrzwsf/AFDUIK8fCKnIV9a6CB0KkrM?dl=0&e=1&preview=Wikipedia_DSA_Audit_Report_2024-25_Public.pdf&rlkey=z0xwzv6e5irwa3b24qg9nj4vu&st=12gpxrxe.

Designated services	Measure Description
	The 2025 Independent Audit of X provided positive conclusions on the platform's implementation of notice and action mechanism requirements under Article 16 of the DSA.[1483]
XNXX	XNXX's reporting infrastructure does not include a dedicated scam reporting category. XNXX indicates that its general content reporting mechanism covers illegal content and content violating its Terms of Service and explicitly includes within its scope phishing and malware as subsets of the broader illegal or policy-violating content category. Users report through the general mechanism regardless of the specific type of violating material being flagged. No further details of the design, placement, or user flow of the reporting mechanism are described in the platform's publicly available documentation. The 2025 Independent Audit of XNXX.com provided a positive conclusion on the platform's implementation of notice-and-action mechanisms under Article 16 DSA.[1484]
XVideos	XVideos describes a general "User Reports (Notice and Action)" system through which users can submit reports about content. Accordingly, users notify the platform of potentially illegal or policy-violating content, and the platform is required to act on such notices. No scam-specific reporting categories, dedicated fraud labels, or further details of the form's structure or user flow are described in the platform's documentation. Scam-related content would be reported through the general notice-and-action pathway. The 2025 Independent Audit of XVideos.com provided a positive conclusion on the platform's implementation of notice and action mechanism requirements under Article 16 of the DSA.[1485] The Independent Audit has comments on the implementation of Art. 16(6).[1486]
Zalando	Zalando reports operating a user-facing reporting mechanism, which allows users to submit notices regarding product-related content – principally content associated with products sold by platform partners. In procedural terms, Zalando claims it has been implementing a unified Notice & Action ticketing system to replace a previously fragmented, spreadsheet-based process, integrating the system with its internal workflows and DSA regulatory requirements. Zalando does not use the term "scam" in describing its reporting mechanism, and no dedicated scam or fraud reporting category is described in its documentation; fraudulent or deceptive product content would fall within the general Notice & Action pathway.

[1483] BDO, X's Digital Services Act (DSA) Report, available at: https://www.dropbox.com/scl/fi/7u4piajjcsdczwk9v0r3p/2025-x-dsa-audit-report.pdf?rlkey=swlo09s7bmmx183fr8ajubms6&st=ulv5zal5&e=1&dl=0.

[1484] Certicom, Independent Audit Report on XNXX.com, available at: https://www.dropbox.com/scl/fi/uoahy5diltdjsn7x4ayrh/XNXX-Independent-Audit-Report-2025.pdf?rlkey=o0r64kjn5ob7iowor047ebswu&st=ldk06ba6&e=1&dl=0.

[1485] Certicom, Independent Audit Report on XVideos.com, available at: https://www.dropbox.com/scl/fi/jmajkhxld16ehp044adtb/2025-Audit-Report.pdf?rlkey=bz20xrrowwn1v57s79baa5z3s&st=27zaly14&e=1&dl=0.

[1486] ibid.

Designated services	Measure Description
	The 2025 Independent Audit of Zalando provided a positive conclusion on the platform's implementation of notice and action mechanism requirements under Article 16(1) DSA.[1487] However, the Independent Audit reached negative conclusions for Articles 16(5) and 16(6).[1488]

[1487] Deloitte, Independent Practitioner's Assurance Report on Zalando SE's compliance with the Digital Services Act, available at: https://www.dropbox.com/scl/fi/n8dnm429o1r17uwbc7lbv/2025-Audit-Report.pdf?rlkey=5dq7gcxsymv1kx6kvrof03xrw&st=8msssumh&e=1&dl=0.

[1488] ibid.

Information on redress

Table 25 - Overview of information on redress as reported by the designated services[1489]

Designated services	Measure Description
AliExpress	AliExpress reports providing users who have encountered fraudulent or misleading products with the ability to submit specific report types such as "guided off-platform transaction" and "account takeover" via the Help Centre's Suspicious Report toggle. For dispute resolution, AliExpress reports operating both after-sales customer service and out-of-court settlement mechanisms, designed to ensure consumer complaints are addressed and resolved in a fair and timely manner.
Amazon Store	Amazon Store reports that it provides the A-to-Z Guarantee to customers who purchase products from third-party Sellers, enabling them to get a full refund for any item that does not arrive in the condition expected or on time. According to Amazon, for purchases made from Amazon Retail, customers have equivalent return and refund rights under the Amazon EU Store return policy. The platform states that it expanded in 2024 the A-to-Z Guarantee to include customer claims for property damage and personal injury caused by defective physical products. Additionally, Amazon indicates that if it identifies that a customer purchased a counterfeit or recalled product, it proactively contacts the customer, informs them that they purchased a counterfeit product, and fully refunds their purchase – without the need for the customer to take any action.
Apple App Store	For EU users, Apple indicates that it provides a link to its DSA redress page, which lists redress options for anyone who has filed an Article 16 Notice via the Content Reports portal and who wants to challenge Apple's decision, as well as redress options for developers and users who want to challenge decisions Apple has taken. Apple states that if a notifier disagrees with an outcome, they have the option to challenge the decision via the Content Reports complaints page.
Bing	No information is provided by Bing in its Report.
Booking.com	Booking.com indicates that if travellers make bookings at properties which are subsequently identified as illegal listings, it removes the illegal property listing and works with the traveller to identify an alternative accommodation. According to the platform, users can raise complaints via various channels, including Customer Service or via the Compliance helpline reporting function. Booking.com states that, given the damage suffered in such incidents is principally financial in nature, the harm is generally more remediable than in other areas where psychological or physical impacts could occur, and that it dedicates significant resources to minimising occurrences and their impact.

[1489] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

Designated services	Measure Description
Google designated services	No information is provided by Google in its Report.
LinkedIn	LinkedIn describes that it has implemented in-product experiences and that it provides resources to remind members that while they are in their job search, they should keep an eye out for signs of potential fraud – including jobs that ask for payment, account credentials, or other highly sensitive personal data; that claim to offer high pay for little work; that give job offers after one remote interview; and that include bad grammar or multiple misspellings. LinkedIn also reports reminding members to research a company, its official website, and its social media accounts before applying, and that it encourages members to report suspicious jobs to LinkedIn. LinkedIn mentions running educational campaigns to increase job seeker awareness about common fraud schemes and that it seeks to empower members to play a proactive role in avoiding scams and to contribute to LinkedIn's efforts to safeguard all members through the reporting of suspicious activities.
Meta designated services	Meta reports developing a library of tools and resources for improved online safety to help educate users, provide guidance about scams (e.g., romance and financial scams), and to encourage users to report content they believe violates its Community Standards and policies. These resources are reportedly available through the Facebook Help Centre and Instagram Help Centre, as well as Meta's Scam Safety Centre and Anti-Scams Hub.
Pinterest	No information is provided by Pinterest in its Report.
Pornhub	No information is provided by Pornhub in its Report.
Shein	No information is provided by Shein in its Report.
Snapchat	Snapchat reports that its Safety Center includes a Safety Resources and Support page that provides users with additional resources, including country-specific information. Snapchat reportedly provides guidance on harms and how to get help in its Safety Center, and offers a summary and explanation of "Fraud and Spam" in its explainer of Harmful, False or Deceptive Practices and its Transparency Report Glossary. Additionally, Snapchat indicates that it has supported the StopThinkFraud campaign on its platform, and that its Safety Center includes a Safety Resources and Support page with country-specific information.
Temu	Temu reports that it operates a Purchase Protection Program which guarantees full refunds for mismatched, damaged, undelivered, late, or lost products. The platform describes that a customer support team is available for users to exercise their statutory rights regarding any orders placed, and that general appeals and complaint mechanisms exist where users affected by Temu’s decisions have a direct avenue to be heard.
TikTok	TikTok reports that its Safety Centre includes resources on a range of topics, including scams.
Wikipedia	No information is provided by Wikipedia in its Report.

Designated services	Measure Description
X	No information is provided by X in its Report.
XNXX	No information is provided by XNXX in its Report.
XVideos	No information is provided by XVideos in its Report.
Zalando	No information is provided by Zalando in its Report.

Friction tools

Table 26 - Overview of scam-relevant friction tools as reported by the designated services[1490]

Designated services	Measure Description
AliExpress	AliExpress describes that it has implemented a friction mechanism within its Instant Messaging (IM) feature whereby external links are detected, and users are warned of associated risks before clicking. According to the platform, this warning prompt introduces a deliberative pause by alerting users to potential risks before they proceed with clicking external links shared through in-platform messaging.
Amazon Store	No information is provided by Amazon Store in its Report.
Apple App Store	No information is provided by Apple App Store in its Report.
Bing	Bing indicates that it deploys Public Service Announcements (PSAs) for certain high-risk query categories, displayed at the top of search results. According to the search engine, these PSAs "highlight authoritative information including reporting and support options, and/or offer clear warnings about potential risks". Bing reports that its safety philosophy also includes in-product indicators and disclosures "such as warnings, disclosure footers, or icons that explain when content has been removed or flagged, and why". The search engine indicates that these mechanisms serve to inform users of safety-related actions and potential risks.
Booking.com	No information is provided by Booking.com in its Report.
Google Play	Google describes one explicit friction tool: Google Play Protect, which automatically scans every app on Android devices with Google Play Services, no matter the source of download, to combat code-level, hidden, and emerging threats. According to Google, this built-in protection scans more than 200 billion apps every day, automatically revokes app permissions for potentially dangerous apps, and displays reminder notifications to remind users that an app installed from an Internet source may not be safe.
Other Google designated services	No information is provided by Google in its Report in relation to its other designated services.
LinkedIn	LinkedIn indicates that it has implemented several friction tools designed to warn users and encourage more reflective interaction. The platform describes that it surfaces a warning and fraud prevention resources to users if its technology detects an attempt to move private conversations away from LinkedIn, which is designed to encourage users to consider the likely authenticity of the people with whom they are engaging. According to its reports, LinkedIn also displays safety reminders to European members who have enabled

[1490] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

Designated services	Measure Description
	certain enhanced safety features if attempts to move private conversations away from the platform are detected in their incoming messages. It is also indicated that the member can click through to view or report the message. LinkedIn also reportedly warns members when photos or videos in Feed or Profiles are detected that may contain sensitive or graphic content; the content will initially be blurred with a warning, giving members control over whether they view this content. Additionally, LinkedIn reports that where its automated systems detect potentially harmful content in messages, depending on whether the sender and recipient have exchanged prior communications, the message will be directed to the recipient's spam folder or be hidden from the recipient by a warning which can be dismissed, giving the recipient the ability to view and report the message to LinkedIn for review if desired.
Meta designated services	Facebook and Instagram report deploying several friction tools designed to protect users from harmful and potentially fraudulent interactions. The platforms describe deploying product interventions with safety notices and prevention features that add friction to the discovery of harmful content. They also indicate that they maintain content interstitials that warn or provide contextual information to users regarding content that, while not policy-violating, may be sensitive, enabling users to decide how to engage with such content. Moreover, Meta describes implementing in-product mechanisms to limit the spread of state-controlled media, including blocking ads, placing content lower in users' feeds, and adding nudges that ask users to confirm they want to share or navigate to content from these outlets. According to Meta, when an interaction is identified as potentially risky or suspicious, the machine-learning-based detection system can trigger various alerts, including displaying warnings to users interacting with suspicious accounts and limiting the ability of flagged accounts to interact with other users.
Pinterest	No information is provided by Pinterest in its Report.
Pornhub	No information is provided by Pornhub in its Report.
Shein	No information is provided by Shein in its Report.
Snapchat	Snapchat reports adopting protective measures to limit teen contact with strangers, including warnings displayed to teens when they first start chatting with someone who may be a stranger. Snapchat reports that the warning mechanism aims to introduce friction when teens begin conversations with strangers.
Temu	Temu reports implementing several friction tools. The platform states that it has added alerts within search results that appear when users enter search terms associated with counterfeit products, providing real-time guidance to promote informed purchasing decisions and protect brands. According to Temu, a recent daily snapshot showed that these alerts were triggered more than 12,000 times, helping users distinguish between genuine and counterfeit products. Additionally, the platform reports using blocking messages within its chat function, whereby various blacklisted terms trigger messages that prevent non-compliant communication. Temu also claims that it adopted a mechanism that blocks and blacklists non-compliant search keywords entered by users, preventing the display of recommended keywords and returning no search results for blacklisted terms.

Designated services	Measure Description
TikTok	TikTok's Systemic Risk Assessment Report does not contain data on friction tools. However, TikTok's publicly available policies mention the introduction of warning labels or prompts for users to pause before sharing unconfirmed content.[1491]
Wikipedia	No information is provided by Wikipedia in its Report.
X	X describes related measures, including restricted reach, rate limiting, and unsafe URL detection, indicating that these work to reduce the impact of misleading activity – including malicious URLs – by reducing impressions and limiting user exposure to such content. X reports that it also operates Community Notes, through which contributing users can provide context and warnings to other users if they identify misleading information or third-party links that may be unsafe, including those that may attempt to scam users.
XNXX	No information is provided by XNXX in its Report.
XVideos	No information is provided by XVideos in its Report.
Zalando	No information is provided by Zalando in its Report.

[1491] TikTok, Integrity and Authenticity, available at: https://www.tiktok.com/safety/en/policies-and-engagement/integrity-authenticity.

Platform policies

Table 27 - Overview of platform-level policies as reported by the designated services[1492]

Designated services	Measure description
AliExpress	AliExpress indicates that its Intellectual Property Rights Protection Rules prohibit and restrict product policies, and merchant compliance rules establish obligations relating to counterfeit goods, fraudulent seller conduct, and product authenticity. AliExpress also reports that additional governance categories addressing concealed counterfeiting and product mis-categorisation specifically target attempts to circumvent platform rules through deceptive listing practices.
Amazon Store	Amazon Store indicates that its Product Listing Rules establish requirements relating to product safety, compliance, authenticity, and seller conduct, while policies governing customer reviews prohibit incentivised, fake, or manipulative reviews. Amazon also reports that marketplace governance is further supported by programmes such as Project Zero, the Amazon Patent Evaluation Express (APEX) programme, and the Counterfeit Crimes Unit, which formalise participation by rights holders and provide dedicated procedures for addressing counterfeit and fraudulent activity.
Apple App Store	Apple App Store states that its App Review Guidelines establish pre-distribution requirements prohibiting deceptive functionality, impersonation, misleading commercial practices, fraudulent transactions, and unlawful conduct. These requirements are reportedly complemented by the Apple Media Services Terms, Submission Guidelines, and Apple Advertising Terms of Service, which prohibit users, developers, and advertisers from engaging in fraudulent, manipulative, or deceptive activity across Apple's ecosystem.
Bing	Bing indicates that its Webmaster Guidelines prohibit practices intended to manipulate search rankings through deceptive or misleading means, while the Microsoft Advertising Policies prohibit fraudulent advertising, phishing, deceptive commercial practices, and the promotion of harmful products or services. These requirements are reportedly complemented by provisions within the Microsoft Service Agreement, including Consumer Protection and Fraud rules, as well as anti-spam and anti-manipulation policies. The Bing Image Creator Terms of Use additionally prohibit the use of generative AI services for fraudulent, deceptive, or misleading purposes and prohibit the removal or alteration of content credentials and provenance information associated with AI-generated content.
Booking.com	Booking.com indicates that its Content Standards and Guidelines establish requirements concerning the accuracy, transparency, and reliability of information presented to travellers. These standards reportedly prohibit content that may mislead, deceive, or confuse users, including inaccurate property information, misleading descriptions, and other content that may distort consumer decision-making during the booking process.

[1492] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

Designated services	Measure description
Google designated services	Google Search Google states that the Misrepresentation Policy, Financial Products and Services Policy, Counterfeit Goods Policy, and Spam Policies for Google Search prohibit phishing, deceptive financial services, counterfeit products, dishonest business practices, and other forms of misleading conduct. Google also claims that its governance measures targeting scaled-content abuse, site-reputation abuse, and expired-domain abuse establish rules intended to prevent manipulation of ranking systems and artificial amplification of deceptive content. YouTube According to its reports, YouTube's content policies, called the Community Guidelines, do not allow scams. Under the deceptive practices and scams policies, YouTube states that it prohibits scam content such as offering cash gifts, "get rich quick" schemes, or pyramid schemes (sending money without a tangible product in a pyramid structure) in videos, comments, and metadata posted by users.[1493] Other Google designated services No information is provided by Google in its Report in relation to its other designated services.
LinkedIn	LinkedIn indicates that its Professional Community Policies prohibit scams and fraud, false or misleading content, deceptive recruitment practices, impersonation, spam, and inappropriate commercial activity. The platform describes these rules as establishing conduct requirements applicable to members, recruiters, advertisers, and organisations operating on the platform.
Meta designated services	Meta describes that the Community Standards, Advertising Standards, Manipulated Media Policy, and policies on Coordinated Inauthentic Behaviour establish platform-wide rules governing scams, fraud, impersonation, deceptive advertising, and misleading synthetic media.
Pinterest	Pinterest reports that its Community Guidelines prohibit scams, deceptive practices, spam, and misleading content, while the platform's advertising and merchant policies establish additional requirements for commercial actors promoting products and services. These rules reportedly govern the authenticity of content, commercial representations, and interactions occurring on the platform, including content intended to mislead users for financial gain.
Pornhub	Pornhub claims that its Terms of Service, Community Guidelines, and uploader-verification requirements establish rules governing the submission of content and user conduct. Pornhub states that its governance measures place particular emphasis on identity verification, consent requirements, and compliance obligations applicable to content uploaders before content may be published on the platform.
Snapchat	Snapchat indicates that its Community Guidelines, Advertising Policies, Creator Monetisation Policies, and Content Guidelines prohibit scams, deceptive commercial activity, and misleading content. Snapchat indicates that its governance requirements extend to generative AI systems through AI-specific Acceptable Use Policies, which establish restrictions on harmful or deceptive uses of AI during

[1493] Google, Tackling scams and fraud together – Google white paper (2024), available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Tackling_scams_and_fraud_together.pdf.

Designated services	Measure description
	development, testing, deployment, and use. Snapchat also states that content classified as engagement bait is designated as Not Eligible for Recommendation, limiting its eligibility for algorithmic amplification.
Shein	Shein reports that its Reviews Policy establishes requirements relating to the authenticity and reliability of user reviews, while the Product Recall Standard Operating Procedure sets out procedures for responding to products presenting safety or compliance concerns. These measures are described by Shein to operate alongside marketplace rules governing counterfeit goods, misleading product information, seller conduct, and product authenticity.
Temu	Temu states that its Platform Rules, merchant governance requirements, product-listing rules, and intellectual-property protection policies establish obligations relating to seller conduct, product authenticity, prohibited products, review integrity, and deceptive commercial practices. Temu also indicates that these rules are supported by merchant compliance requirements that define responsibilities throughout the seller lifecycle and establish standards for product representations and marketplace behaviour.
TikTok	TikTok claims that its Community Guidelines prohibit scams, impersonation, deceptive financial schemes, and harmful digital forgeries. Policies governing synthetic and AI-generated media reportedly establish disclosure and authenticity requirements intended to reduce the risk of users being misled by manipulated or artificially generated content.
Wikipedia	Wikipedia reports that the Verifiability Policy, Reliable Sources Guideline, Conflict of Interest Guideline, and Paid-Contribution Disclosure requirements establish procedural safeguards intended to ensure information can be independently verified and that users disclose interests that may affect content creation or editing.
X	X reports that its Rules prohibit platform manipulation and spam, deceptive identities, impersonation, and fraudulent behaviour. These rules are reportedly supplemented by the Platform Manipulation and Spam Policy, which describes how to address coordinated attempts to artificially amplify content or mislead users, and the Synthetic and Manipulated Media Policy, which establishes requirements relating to deceptive or misleading synthetic content. The platform also claims to maintain policies governing authenticity, advertising conduct, and coordinated activity intended to preserve the integrity of interactions on the service.
XNXX	XNXX reports that its Terms of Service, content policies, and uploader requirements establish rules prohibiting illegal content, unauthorised content, and other forms of prohibited activity. XNXX also states that governance measures include user obligations relating to content ownership, legality, and compliance with platform rules as conditions for publication and continued access to platform services.
XVideos	XVideos reports that its Terms of Service, content-upload rules, and content policies establish requirements relating to the legality, ownership, and permissibility of uploaded content. These governance measures reportedly define prohibited categories of content and establish compliance obligations applicable to users and content uploaders operating on the platform.
Zalando	Zalando describes the Partner Program Terms and Conditions, Code of Conduct, product-compliance requirements, and review-related standards as establishing obligations for marketplace partners relating to product authenticity, consumer protection, accurate product information, and responsible commercial practices. Zalando indicates that these requirements govern merchant participation on the

Designated services	Measure description
	marketplace and establish standards intended to ensure the reliability of product listings, reviews, and marketing communications presented to consumers.

Cooperation with third parties

Table 28 - Overview of cooperation with third parties as reported by the designated services[1494]

Designated services	Measure description
AliExpress	AliExpress reports that intellectual-property rights holders participate in the identification and reporting of counterfeit and infringing listings through dedicated rights-protection mechanisms. AliExpress also reports that external inspection providers support review processes for listings and user-generated content identified as potentially non-compliant.
Amazon Store	Amazon Store claims that Project Zero enables participating brands to directly remove counterfeit listings and contribute infringement signals to platform integrity systems. Amazon also reports that its Patent Evaluation Express (APEX) programme incorporates independent patent attorneys into patent-dispute resolution processes. Amazon indicates that the Counterfeit Crimes Unit coordinate investigations with rights holders and law-enforcement authorities targeting counterfeit and fraudulent networks operating both on and off the platform.
Apple App Store	No specific information is provided by Apple App Store in its Report.
Bing	Bing reports that its participation in the Coalition for Content Provenance and Authenticity (C2PA) supports the development and implementation of shared standards for content credentials, provenance information, and AI-generated content. Bing also indicates that fraud investigations combine platform signals with intelligence from external security researchers and industry partners involved in identifying evolving scam techniques and fraudulent infrastructure.
Booking.com	No specific information is provided by Booking.com in its Report.
Google designated services	Google reports that the Face Forensics initiative, developed jointly with Google/Jigsaw and external researchers, provides a large-scale dataset of manipulated images and video frames used to train and evaluate deepfake-detection systems.[1495] Google also indicates that collaboration with researchers contributes to the identification of emerging manipulation techniques and the development of content-

[1494] Based on AliExpress, Amazon Store, App Store, Bing, Booking.com, Facebook, Google Maps, Google Play, Google Search, Google Shopping, Instagram, LinkedIn, Pinterest, Pornhub, Shein, Snapchat, Temu, TikTok, Wikipedia, X, XNXX, XVideos, YouTube, Zalando 2025 Risk Assessment Reports.

[1495] Nick Dufour and Andrew Gully, Contributing Data to Deepfake Detection Research (2019), available at: https://research.google/blog/contributing-data-to-deepfake-detection-research/; Andreas Rössler, Davide Cozzolino, Luisa Verdoliva, Christian Riess, Justus Thies, and Matthias Nießner, FaceForensics++: Learning to Detect Manipulated Facial Images (2019), available at: https://www.researchgate.net/publication/330672957_FaceForensics_Learning_to_Detect_Manipulated_Facial_Images.

Designated services	Measure description
	authenticity assessment tools.[1496] Further, Google indicates that it is working with financial institutions and regulators to raise user literacy with educational safety guides and toolkits.[1497]
LinkedIn	No specific information is provided by LinkedIn in its Report.
Meta designated services	Meta reports that researcher-access programmes and transparency tools, including the Meta Ad Library, enable external scrutiny of advertising activity and systemic platform risks. Meta indicates that cooperation with law-enforcement authorities supports the identification and disruption of organised scam operations and criminal networks operating across multiple jurisdictions. Meta announced the Llama Defenders Programme, which seeks to provide partner organisations and developers with access to a range of AI-based security tools designed to address threats including fraud, phishing, and scam activity.[1498] Meta also reports operating a Trusted Partner Programme.[1499]
Pinterest	Pinterest indicates that external experts specialising in specific harm domains provide intelligence on emerging abuse patterns and behavioural trends. The platform describes that signals derived from these partnerships may be incorporated into moderation systems, policy development processes, and targeted enforcement initiatives.
Pornhub	No specific information is provided by Pornhub in its Report.
Snapchat	Snapchat reports that advertiser-verification, domain-assessment, and trust-and-safety processes incorporate information from external providers involved in assessing advertiser legitimacy and identifying deceptive destinations. Participation in wider industry safety initiatives is reported by Snapchat as supporting the identification of emerging platform-integrity risks.
Shein	No specific information is provided by Shein in its Report.
Temu	According to Temu, intellectual-property rights holders may submit infringement complaints and contribute information regarding counterfeit or infringing products through dedicated rights-protection channels. Temu also indicates that external stakeholders can report marketplace violations through formal complaint mechanisms.

[1496] ibid.

[1497] Google, Tackling scams and fraud together – Google white paper (2024), available at: https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Tackling_scams_and_fraud_together.pdf.

[1498] Meta, Sharing new open source protection tools and advancements in AI privacy and security (2025), available at: https://ai.meta.com/blog/ai-defenders-program-llama-protection-tools/.

[1499] Meta, Measuring Performance of the Trusted Partner Channel (2025), available at: https://transparency.meta.com/governance/tracking-impact/measuring-performance/.

Designated services	Measure description
TikTok	TikTok reports that its cooperation with researchers, fact-checking organisations, civil-society organisations, and industry partners contributes to the identification of emerging risks, deceptive practices, manipulated media, and coordinated harmful activity.
Wikipedia	Wikipedia indicates that its community governance relies on collaboration between volunteer editors, administrators, Wikimedia affiliates, researchers, and that external organisations contribute expertise on content quality, misinformation, and platform integrity risks.
X	X reports that its cooperation with external researchers, industry stakeholders, and relevant authorities contributes to efforts addressing platform manipulation, coordinated activity, and other integrity-related threats.
XNXX	XNXX reports on its cooperation with law enforcement agencies, including responding to lawful requests for information and cooperating with relevant authorities.
XVideos	XVideos reports on its cooperation with law enforcement authorities and NGOs as part of its approach to addressing illegal content and platform risks.
Zalando	Zalando indicates that rights holders, marketplace partners, and competent authorities contribute information relating to counterfeit products, intellectual-property infringements, and marketplace-compliance concerns through dedicated reporting and cooperation mechanisms.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

Publications Office
of the European Union
Law | Data | Publications