

ARTICOLI

Le frodi nei pagamenti elettronici (contesto economico e regole di settore)

FULVIO GIGLIOTTI

Professore Ordinario di Diritto privato
Università degli Studi Magna Graecia di Catanzaro

Dialoghi di Diritto dell'Economia

Rivista diretta da

Danny Busch, Raffaele Lener, Roberto Natoli, Andrea Sacco Ginevri,
Filippo Sartori, Antonella Sciarrone Alibrandi

Direttore editoriale

Andrea Marangoni

Coordinatore editoriale

Francesco Petrosino

Direttori di area

Attività, governance e regolazione bancaria

Prof. Alberto Urbani, Prof. Diego Rossano, Prof. Francesco Ciraolo, Prof.ssa Carmela Robustella, Prof. Gian Luca Greco, Prof. Federico Riganti, Dott. Luca Lentini, Dott. Edoardo Cecchinato, Dott.ssa Angela Galato

Mercato dei capitali finanza strutturata

Prof. Matteo De Poli, Prof. Filippo Annunziata, Prof. Ugo Malvagna, Prof. Alain Pietrancosta, Prof.ssa Paola Lucantoni, Dott.ssa Anna Toniolo

Assicurazioni e previdenza

Prof. Paoloefisio Corrias, Prof. Michele Siri, Prof. Pierpaolo Marano, Prof. Giovanni Maria Berti De Marinis, Prof. Robert Merkin, Prof.ssa Kyriaki Noussia, Dott. Massimo Mazzola

Contratti di impresa, concorrenza e mercati regolati

Prof.ssa Maddalena Rabitti, Prof.ssa Michela Passalacqua, Prof.ssa Maddalena Semeraro, Prof.ssa Mariateresa Maggiolino, Dott. Gianpaolo Panetta

Diritto della crisi di impresa e dell'insolvenza

Prof. Aldo Angelo Dolmetta, Prof. Gianluca Mucciarone, Prof. Francesco Accettella, Dott. Antonio Didone, Prof. Alessio di Amato, Prof. Ignacio Tirado

Fiscalità finanziaria

Prof. Andrea Giovanardi, Prof. Nicola Sartori, Prof. Francesco Albertini

Istituzioni dell'economia e politiche pubbliche

Prof.ssa Michela Passalacqua, Prof. Francesco Moliterni, Prof. Giovanni Luchena, Dott.ssa Stefania Cavaliere, Dott. Lorenzo Rodio Nico

Criteri di Revisione

I contributi proposti alla Rivista per la pubblicazione sono sottoposti a una previa valutazione interna da parte della Direzione o di uno dei Direttori d'Area; il quale provvede ad assegnare il contributo a un revisore esterno alla Rivista, selezionato, *rationes materiae*, fra professori, ricercatori o assegnisti di ricerca.

La rivista adotta il procedimento di revisione tra pari a singolo cieco (*single blind peer review*) per assicurarsi che il materiale inviato rimanga strettamente confidenziale durante il procedimento di revisione.

Qualora il valutatore esprima un parere favorevole alla pubblicazione subordinato all'introduzione di modifiche, aggiunte o correzioni, la Direzione si riserva di negare la pubblicazione dell'articolo. Nel caso in cui la Direzione decida per la pubblicazione, deve verificare previamente che l'Autore abbia apportato le modifiche richieste dal Revisore.

Qualora il revisore abbia espresso un giudizio negativo, il contributo può essere rifiutato oppure inviato, su parere favorevole della maggioranza dei Direttori dell'area competente *rationes materiae*, a un nuovo revisore esterno per un ulteriore giudizio. In caso di nuovo giudizio negativo, il contributo viene senz'altro rifiutato.

Le frodi nei pagamenti elettronici (contesto economico e regole di settore)

FULVIO GIGLIOTTI

Professore Ordinario di Diritto privato
Università degli Studi Magna Graecia di Catanzaro

* SOMMARIO: 1. Premessa. – 2. I pagamenti digitali: il contesto economico. – 3. Le operazioni dispositive e i pagamenti con carta. – 4. Le tipologie prevalenti di frode. – 5. L'assetto normativo e gli obblighi delle parti. – 6. Responsabilità e rimborsi: gli orientamenti ABF. – 7. Considerazioni conclusive e prospettive evolutive.

1. Premessa

L'evoluzione tecnologica contemporanea e la spinta (ormai incessante) verso la digitalizzazione⁰¹ – peraltro favorita (in termini generali e globali) anche dalla recente disavventura pandemica mondiale⁰² – hanno radicalmente trasformato il panorama economico globale⁰³, modificando le abitudini di consumo e accelerando la transizione verso una *cashless society*, sebbene non ancora compiutamente realizzata: in questo conte-

* Il presente contributo riproduce – omesse le parole di circostanza e con l'aggiunta delle note e alcuni adattamenti e aggiornamenti (anche bibliografici) – la relazione presentata al Convegno su “Trasparenza bancaria e regolazione del mercato. Il ruolo dell'ABF” – Catanzaro, 27 marzo 2026. I dati statistici riportati sono stati aggiornati (rispetto a quelli riferiti in relazione) – ove possibile – agli ultimi resi disponibili alla data di consegna del testo scritto della relazione. I contenuti esposti esprimono opinioni personali dell'Autore e non sono in alcun modo riconducibili all'Arbitro Bancario Finanziario di cui lo stesso fa parte.

01 In proposito v., in termini generali: V. CODELUPPI, *Mondo digitale*, Milano, Laterza, 2022; P. BENANTI, *Digital age. Teoria del cambio d'epoca. Persona, famiglia e società*, Roma, San Paolo edizioni, 2020; D. MANCA, G. GHIDINI, A. MASSOLO, *La nuova civiltà digitale. L'anima doppia della tecnologia*, Milano, Solferino, 2020.

02 Per tutti v. T.E. CHOWDHURY-R. CHOWDHURY- M. RAHMAN-A- RAHMAN SUNNY, *From Crisis to Opportunity: How Covid-19 Accelerated the Global Shift to Online Business*, in *Pathfinder of Research*, 2022, 13 ss.

03 Per i riflessi, specificamente, sul settore bancario v., assai di recente, E. Camilleri-M. Maugeri (a cura di), *Contratto e concorrenza nel mercato bancario. Le sfide del XXI secolo*, Torino, Giappichelli, 2026.

sto, i sistemi di pagamento elettronici (in senso ampio)⁰⁴ – dalle carte di debito e credito ai portafogli digitali, fino alle transazioni tramite *smartphone* e valute virtuali (pur, naturalmente, nella diversità, secondo i casi, delle singole discipline di riferimento) – non rappresentano più una semplice alternativa al denaro contante, ma il vero e proprio motore del commercio moderno, sia *on line* che nei canali fisici.

Naturalmente, se, da un lato, questa rivoluzione ha garantito rapidità, efficienza e tracciabilità non comparabili con quelle delle transazioni tradizionali, dall'altro – però – ha anche necessariamente ridefinito confini e modalità operative della criminalità finanziaria, spostando l'asse delle attività illecite dal piano fisico a quello digitale; e così, alle tradizionali attività criminose, quali furti e rapine, si sono progressivamente sostituite – in modo preponderante – le frodi informatiche e gli inganni digitali⁰⁵, dando consistenza sempre più preoccupante a situazioni e tecniche decettive assai fluide, globali e in costante mutamento: invero, le frodi nei pagamenti elettronici non si limitano più – ormai – al furto di identità o alla clonazione delle carte, ma sfruttano tecniche particolarmente sofisticate, che combinano attacchi cybernetici avanzati (come *malware* e violazioni di *database*) con pratiche di ingegneria sociale (c.d. *social engineering*) per la manipolazione psicologica degli utenti, attraverso (come meglio si dirà) tecniche di *phishing*, *vishing*, *smishing* e altre (ben più insidiose) modalità decettive.

La vulnerabilità principale del sistema si è così spostata dall'infrastruttura tecnologica

04 In argomento v., ad es.: S. CHISHTI-T. CRADDOCK- R. CORTNEIDEG- M. ZACHARIADIS, *Il manuale della PayTech. Guida ai pagamenti digitali per imprenditori, manager e operatori della finanza*, Milano, ed Apogeo, 2021; M.C. Paglietti-M. C. Evangelisti (a cura di), *Innovazione e regole nei pagamenti digitali. Il bilanciamento degli interessi nella PSD2*, Roma, ed RomaTre-press, 2020; G. ARANGÜENA-D. JEGERSON, *I pagamenti elettronici. Dal baratto ai portafogli digitali*, e-book, goWare, 2015. V., altresì, il *Libro bianco su Fintech e pagamenti digitali*, a cura di M. Guerriero, accessibile direttamente in rete, all'indirizzo Internet https://www.startmag.it/wp-content/uploads/Fintech_Web-260218.pdf.

05 Con una significativa accentuazione e consolidazione, evidentemente, nel periodo pandemico, atteso che – come rilevato da E. LUCCHINI GUASTALLA, *Strumenti di pagamento e rimedi*, in E. Camilleri-M. Maugeri (a cura di), *Contratto e concorrenza nel mercato bancario*, cit., 89 – «le restrizioni alla mobilità imposte durante l'emergenza pandemica da Covid-19 hanno significativamente ridotto le occasioni di sottrazione fisica degli strumenti (si pensi, emblematicamente, ai furti perpetrati sui mezzi pubblici), inducendo gli autori degli illeciti a ricercare strategie alternative».

Sul tema delle frodi nei pagamenti digitali v., assai di recente: G. GIUSTI, *La responsabilità degli intermediari finanziari nelle nuove frodi digitali*, in ius.lefebvrejuffre.it, 6 maggio 2026; G. LEMME, *Servizi di pagamento e tutela delle persone vulnerabili*, in *Riv. dir. bancario*, 2026, 1 ss. V., altresì, per un efficace quadro di sintesi, A. GENOVESE, *L'utilizzo fraudolento degli strumenti di pagamento*, in F. Greco-G. Liace (dir.), *Diritto bancario (I trattati Giuffrè). Il. Informazione, trasparenza e tutela*, Milano, 2025, 655 ss.; F. CIVALE, *Frodi nelle operazioni di pagamento e profili di responsabilità. Orientamenti ABF ed evoluzione normativa*, in www.diritto bancario.it, 9 maggio 2024.

all'anello umano⁰⁶; affrontare il tema delle frodi nei pagamenti digitali significa, quindi, prospettare una sfida multidimensionale: da una parte, infatti, vi è la necessità (sul piano normativo e regolatorio) di implementare discipline rigorose (come le direttive europee PSD2 e, prossimamente, PSD3; nonché il regolamento c.d. PSR⁰⁷) e tecnologie di difesa all'avanguardia, quali (quelle che impiegano) l'intelligenza artificiale e la crittografia biometrica; dall'altra, tuttavia, emerge anche l'urgenza di promuovere una più solida cultura della sicurezza digitale tra i consumatori⁰⁸. E in questa dimensione, il vero obiettivo regolatorio del settore finanziario moderno non è tanto l'azzeramento del rischio – obiettivo che, ragionevolmente, appare abbastanza utopistico in un ecosistema necessariamente interconnesso – quanto, auspicabilmente, il raggiungimento del miglior equilibrio possibile tra la garanzia del massimo livello di protezione edificabile e la salvaguardia di quella immediatezza e semplicità d'uso che rende i pagamenti elettronici ormai assolutamente indispensabili.

2. I pagamenti digitali: il contesto economico

Un rapido sguardo al mercato di riferimento conferma immediatamente, d'altra parte, la necessità di interventi regolatori specifici, diretti ad arginare, per quanto possibile, situazioni di abuso fraudolento, compatibilmente con l'esigenza di non compromettere la (crescente) diffusione del fenomeno dei pagamenti digitali.

06 Come rileva G. LEMME, *Servizi di pagamento e tutela delle persone vulnerabili*, cit., 20, «l'età e la natività digitale non si sono rivelate sufficienti a creare un "porto sicuro", nel quale l'esposizione al rischio sia trascurabile. Se è certamente vero che gli anziani rimangono più facilmente vittima di frodi, il mutevole quadro tecnologico (e la fantasia dei truffatori) provocano spesso problemi anche per i clienti più giovani».

07 Sull'evoluzione delle diverse discipline di matrice europea – dalla c.d. PSD, direttiva 2007/64/CE del Parlamento europeo e del Consiglio, adottata in data 13 novembre 2007, avente ad oggetto la disciplina dei servizi di pagamento nel mercato interno (su cui, ad es., S. PAGLIANTINI, *Il nuovo regime della trasparenza nella direttiva sui servizi di pagamento*, in *Contratti*, 12, 2009, 1158 ss.) alla PSD2, direttiva UE 2015/2366 del Parlamento europeo e del Consiglio, emanata il 25 novembre 2015 (per la quale v., ex multis: M. SEMERARO, *Modelli di responsabilità e private enforcement: appunti su PSD2 e operazioni di pagamento non autorizzate*, in *Riv. dir. bancario*, 2022, 825 ss.; S. VANINI, *L'attuazione in Italia della seconda direttiva sui servizi di pagamento nel mercato interno: le innovazioni introdotte dal d.lgs., 15 dicembre 2017, n. 218*, in *Nuove leggi civ. comm.*, 2018, 839 ss.); fino alla recente proposta di terza direttiva (c.d. PSD3, del 28 giugno 2023, COM(2023) 366 final, sulla quale v., per tutti, P. MIRTO, *Trasparenza nei pagamenti elettronici e direttiva PSD3: evoluzione normativa, impatti sistemici e prospettive regolatorie*, in *Riv. Dir. risparmio*, 2025, 3 ss.; e, più di recente, per una informazione di sintesi, H. TORREANI, *PSD3: Europe's new payments regulation*, in <https://www.payplug.com/blog/psd3/>) nonché alla proposta di regolamento (PSR) del Parlamento europeo e del Consiglio relativo ai servizi di pagamento nel mercato interno, che modifica il regolamento UE 2010/1093 del 28 giugno 2023 – v., ora, M. RISPOLI FARINA, *L'evoluzione normativa dei servizi di pagamento in un contesto concorrenziale*, Roma, TAB ediz., 2026.

08 Di particolare rilievo, nella prospettiva segnalata, l'azione di educazione finanziaria condotta da Banca d'Italia, su cui v. <https://www.bancaditalia.it/compiti/tutela-educazione/educazione-finanziaria/index.html>.

Secondo gli ultimi dati diffusi dall'*Osservatorio sui pagamenti innovativi* del Politecnico di Milano⁰⁹, in Italia il 45% circa dei consumi passa, ormai, da strumenti elettronici (mentre banconote e monete si fermano al 38%); e, nel 2025, i pagamenti digitali hanno raggiunto un volume complessivo pari a 518 miliardi di euro, in crescita del 7% rispetto al 2024¹⁰.

D'altra parte, con oltre 3,5 milioni di POS installati¹¹, i pagamenti *contactless* costituiscono, sicuramente, la parte più significativa dei pagamenti innovativi (circa il 90% delle transazioni in negozio); ma anche i pagamenti con digitazione del PIN e altre modalità (alcune delle quali particolarmente innovative, come pagamenti attraverso *smartwatch*, oggetti "connessi" alla rete, *wallet* digitali) hanno ormai acquisito sempre maggiore diffusione¹².

In un simile scenario è ben chiaro che anche il mercato delle frodi – possibili, come meglio si dirà a breve (*infra*), con diversi mezzi, taluni dei quali anche assai insidiosi e sofisticati – ha finito per assumere proporzioni rilevanti. In particolare, secondo recenti rilevazioni statistiche, il valore delle transazioni fraudolente con carte di pagamento all'interno dell'area c.d. SEPA (acronimo la cui traduzione indica l'Area unica dei pagamenti in euro, alla quale aderiscono tutti i paesi dell'UE e alcuni altri al di fuori dell'U-

09 Tutti i riferimenti analitici di seguito considerati, nel testo e nelle note, possono essere reperiti visitando il sito <https://www.osservatori.net/innovative-payments/>. Per maggiori dettagli si rinvia al Report dell'Osservatorio su "*I pagamenti digitali in Italia nel 2025*", in <https://www.osservatori.net/report/innovative-payments/pagamenti-digitali-italia-2025/>

10 Nel corso del 2024 – per la prima volta in Italia – i pagamenti digitali hanno superato il movimento di contanti, facendo registrare transazioni per un valore complessivo di circa 481 miliardi di euro, pari al 43% circa dei consumi (solo il 41% in contanti; e il rimanente 16% con bonifici, addebiti in conto e assegni). Solo 5 anni prima, nel 2019, la percentuale era ferma al 29%, ed è stata in costante crescita dal 2020. Il *Rapporto 2025* (primo semestre) dell'Osservatorio segnala anche che cresce ovunque il peso dei pagamenti istantanei da conto a conto: ad es., in Brasile, nel terzo trimestre del 2025, Pix ha processato 7,9 miliardi di transazioni P2B, in crescita del +13%, mentre le carte si sono fermate a 11,6 miliardi, con una lieve crescita del +4%; in India, a dicembre 2025, UPI ha superato 21,6 miliardi di transazioni, in crescita del +29% rispetto all'anno precedente, arrivando a rappresentare l'86% delle transazioni digitali del Paese.

11 Rileva ancora il Report 2025 che il parco POS conta ora 3,6 milioni di terminali, grazie, in particolare, agli Smart POS, che rappresentano il 19% del totale. I *software POS* arrivano a circa 165 mila unità, segnando un'evoluzione importante verso punti cassa sempre più *software-based*.

12 Cfr., in proposito, P. GIANURCO-E. DONEDA, *Pagamenti digitali: in Italia nel 2025 il 45% dei consumi è stato regolato tramite strumenti elettronici*, in <https://www.deloitte.com/it/it/blog/pagamenti-digitali-italia-2025.html>: «nel 2025 il 45% dei consumi in Italia è stato regolato tramite strumenti elettronici, a fronte di un utilizzo del contante che si ferma al 38%»; e nello stesso anno «i pagamenti *contactless* – effettuati tramite carta, *smartphone* o *wearable* – hanno raggiunto i 323 miliardi di euro, confermandosi come modalità prevalente nei punti vendita fisici».

Secondo l'analisi condotta (su 1.800 consumatori italiani) dall'Osservatorio – in collaborazione con Ipsos Doxa – il 96% degli italiani possiede almeno una carta (e l'Osservatorio stima che circa 14 milioni di italiani abbiano pagato con *smartphone* o *wearable* nell'ultimo anno; con una crescita significativa (di circa +4 milioni) rispetto al 2024.

nione) ha toccato gli 1,8 miliardi di euro all'anno¹³: in questo contesto, il 73% delle frodi, per un totale di 1,32 miliardi di euro, è avvenuto sui pagamenti da remoto, come, ad es., quelli negli acquisti *on line*¹⁴.

A febbraio 2026, Banca d'Italia ha pubblicato il "*Rapporto sulle operazioni di pagamento fraudolente in Italia - I semestre 2025*" (d'ora in poi, *Rapporto Banca d'Italia 2026*), nel quale è stato analizzato, come di consueto, l'andamento delle frodi nei pagamenti digitali (periodo considerato: primo semestre 2022-primo semestre 2025): e da tale documento emerge una tendenziale stabilità delle truffe legate ai pagamenti con carte (0,018%) ed ai prelievi presso gli sportelli ATM (0,01%), mentre è risultato in diminuzione (0,043% a fronte del precedente 0,059%) – rispetto al secondo semestre 2024 – il tasso di frode legato all'uso dei bonifici istantanei. Più in generale, comunque, le operazioni di pagamento a distanza sono rimaste più esposte al rischio di frodi (peraltro, più consistenti anche con riferimento all'importo della singola operazione fraudolenta); e, soprattutto, è stata riscontrata una maggiore incidenza delle frodi per le operazioni transfrontaliere rispetto a quelle nazionali¹⁵.

Quanto alle modalità realizzative delle frodi, poi, rileva il *Rapporto* che le frodi c.d. "da manipolazione del pagatore" – cioè, quelle che sfruttano informazioni sul cliente, raccolte con tecniche di ingegneria sociale (inducendolo a disporre volontariamente un pagamento verso un beneficiario fraudolento) – rimangono la tipologia prevalente nelle operazioni con bonifico, con tendenza all'aumento (sebbene sia stata rilevata, per altro verso, una riduzione dell'incidenza statistica per le carte di pagamento e la moneta elettronica) e un'incidenza del 74% in valore (da 69% dello scorso anno) e del 64% in numero (da 59%): e si tratta, evidentemente, di una tipologia di frode molto insidiosa (che

13 Cifra che può sembrare molto alta ma che, in realtà, corrisponde solo allo 0.041% del valore di tutte transazioni.

14 Per una ricognizione dell'andamento delle frodi in materia, seppure ormai datata di qualche anno, v. lo studio (per Banca d'Italia) di G. ARDIZZI-E. BONIFACIO-L. PAINELLI, *Le frodi con carte di pagamento: andamenti globali ed evidenze empiriche sulle frodi online in Italia*, in https://www.bancaditalia.it/pubblicazioni/qef/2020-0562/QEF_562_20.pdf.

15 Più analiticamente, il tasso di frode – cioè l'incidenza del valore delle transazioni fraudolente sul valore totale delle operazioni di pagamento – è di 12 casi ogni centomila operazioni (ovvero un tasso dello 0,012% in numero) e 3 euro ogni centomila euro transati (corrispondente a un tasso dello 0,003% in valore), con differenze significative, però, tra i diversi strumenti di pagamento. In particolare, i pagamenti con moneta elettronica (soprattutto carte prepagate) presentano tassi di frode superiori rispetto alle altre carte e in aumento rispetto allo stesso semestre dell'anno precedente (0,031% in valore, da 0,027%; 0,027% in numero, da 0,023%); anche i bonifici fraudolenti (quelli istantanei, in particolare) risultano tendenzialmente piuttosto diffusi (0,043% in valore e 0,019% in numero), ma in significativa riduzione rispetto al semestre precedente (0,059% in valore; 0,028% in numero): e la riduzione, si nota, può essere stata influenzata dal rafforzamento delle misure di prevenzione e di sensibilizzazione della clientela attuate dai PSP in relazione all'entrata in vigore della *Instant Payment Regulation* (IPR-Regolamento (UE) 2024/886, entrato in vigore il 9 gennaio 2025, che ha previsto, tra l'altro, che i PSP adottino un servizio per garantire la verifica dell'IBAN del beneficiario al quale il pagatore intende inviare un bonifico (cd. *Verification Of Payee*, VOP), con misura resa obbligatoria dal 9 ottobre 2025).

riesce ad essere attuata pur in presenza di presidi di autenticazione forte del cliente: *infra*, § 5), la quale – a differenza delle frodi cd. “non autorizzate” (per es., la clonazione di carte di pagamento) – non consente l’attivazione automatica dei meccanismi di rimborso previsti dalla normativa vigente, rendendo quindi più difficile, per l’utente, il recupero delle somme indebitamente sottratte.

3. Le operazioni dispositive e i pagamenti con carta

Nel contesto economico contemporaneo – come ciascuno può agevolmente constatare da sé – le transazioni commerciali quotidiane ben raramente vengono regolate per contanti, essendo ormai di gran lunga prevalente l’impiego di carte di pagamento (o, in minor misura, di altri strumenti innovativi), utilizzate materialmente, presso il punto di vendita fisico, ovvero “a distanza” (cioè in operazioni dispositive *on line*, a mezzo *Internet*)¹⁶; e in proposito, per quanto – ovviamente – utilizzi abusivi siano ben possibili anche a seguito della materiale apprensione dello strumento di pagamento¹⁷, sono soprattutto le operazioni “a distanza” a rimanere maggiormente esposte al rischio frode, come

¹⁶ Si devono tenere distinte, in particolare, tre diverse tipologie di carte di pagamento: le *carte di credito* (come, ad es., Visa, American Express, etc.), il cui utilizzo comporta che il pagamento attraverso la carta avviene utilizzando la linea di credito concessa dall’emittente all’utilizzatore della carta; le *carte di debito* (i cui circuiti di funzionamento più noti sono Bancomat e Maestro), le quali permettono, invece, di utilizzare direttamente i fondi nella disponibilità dell’utilizzatore sul proprio conto di pagamento, associato alla carta; le *carte prepagate*, il cui utilizzo presuppone il preventivo “caricamento”, sulla carta, della provvista necessaria all’utilizzo della carta.

In ogni caso, comunque, le carte di pagamento sono emesse da un intermediario autorizzato (il c.d. emittente), che, normalmente, coincide con lo stesso intermediario che detiene il conto del cliente, nel caso di carte di debito (mentre nelle carte di credito l’emittente è solitamente soggetto diverso da quello che detiene il conto del cliente; nessun conto, invece, occorre per richiedere e utilizzare una carta prepagata). In concreto, poi, l’utilizzo della carta può avvenire attraverso il suo impiego fisico o materiale (come nei pagamenti a mezzo POS fisso, acronimo di *point of sale*, letteralmente: punto di vendita), oppure – e ormai ben più frequentemente – attraverso l’impiego di un dispositivo elettronico e specifiche applicazioni (come, ad es. un cellulare e le app per il funzionamento del servizio, seguendo le modalità indicate per l’impiego dello strumento), nel caso di acquisti attraverso siti *e-commerce*. In ambedue i casi, in realtà, c’è, in effetti, un terzo soggetto (c.d. convenzionatore o *acquirer*, che è colui che gestisce il POS, fisico o virtuale, utilizzato per la transazione). In pratica, quando il cliente inserisce i dati della carta per procedere al pagamento, l’*acquirer* inoltra la richiesta di transazione al circuito di competenza, che identifica l’emittente della carta, il quale ultimo verifica ed elabora la transazione, autorizzando l’addebito del corrispondente importo sul conto della carta, a questo punto, il circuito conferma l’operazione all’*acquirer*, che – a sua volta – la trasmette all’infrastruttura di cassa del commerciante, il quale può quindi erogare il bene o il servizio negoziati (il tutto avviene, naturalmente, in tempo reale).

¹⁷ «La c.d. “plastica”, secondo la terminologia invalsa nella prassi bancaria», come sottolinea E. LUCCHINI GUASTALLA, *Strumenti di pagamento e rimedi*, cit., 89.

testimoniato dalle evidenze statistiche¹⁸. Peraltro, pur a fronte di una maggior frequenza statistica (ma non dell'importo complessivo¹⁹) del numero di frodi²⁰, «la maggior parte del valore delle perdite» – sostenuta, invece, dagli utenti nel caso dei bonifici e dei prelievi da ATM – «grava principalmente sui PSP – dell'ordinante o del beneficiario – nel caso delle carte di pagamento e della moneta elettronica», rimanendo a carico dell'utente un volume pari a circa il 42% in caso di carte di pagamento (35% per la moneta elettronica), laddove la quota delle perdite a carico dell'utente sale addirittura al 91% circa in caso di bonifici fraudolenti²¹.

In linea di massima, comunque, nessuna operazione dispositiva resa possibile dalle tecnologie attualmente disponibili è esente da rischi di utilizzo fraudolento, ancorché (come sopra anticipato, § 2) la relativa consistenza statistica costituisca, tutto sommato, una frazione non realmente allarmante rispetto al totale delle operazioni poste in essere sul mercato (sebbene – specialmente a causa della frustrazione che comporta per chi ne rimane, occasionalmente, vittima – comunque tale da non poter essere trascurata, specialmente in vista della necessità di garantire e preservare la tendenza alla crescente utilizzazione di pagamenti alternativi all'uso del contante, sempre meno adatto alla tipologia e frequenza delle transazioni commerciali caratteristiche di una società contemporanea).

18 Come rilevato nel *Rapporto Banca d'Italia 2026* (pp. 9 s.), «per le carte di pagamento, le operazioni “a distanza” (pagamenti effettuati via *internet*) risultano significativamente più rischiose rispetto a quelle “non a distanza” (pagamenti effettuati presso il punto vendita fisico). Nel primo semestre del 2025, il tasso di frode per le operazioni “a distanza” (0,065% in valore; 0,048% in numero) è oltre dieci volte superiore a quello delle operazioni “non a distanza” (0,006% in valore; 0,003% in numero), sebbene il divario si sia progressivamente ridotto negli ultimi semestri. In termini di incidenza relativa, le frodi sui pagamenti con carte utilizzate *on line* (ad esempio, sui siti *e-commerce*) rappresentano il 73% del valore e il 77% del numero complessivo delle frodi, pur a fronte di una quota maggioritaria di operazioni di pagamento effettuate presso punti di vendita fisici (80% in valore e 85% in numero)».

Per un'analisi specifica del rischio frode con riguardo alle carte di pagamento v. M. D'AMATO-P. FINALDI RUSSO-R. SANTIONI-L. TOMASSETTI, *Il rischio di frode sulle carte di pagamento: un'analisi del mercato italiano nel periodo 2015-24*, in *Questioni di Economia e Finanza (Occasional papers)*, n. 986 (2025), a cura di Banca d'Italia.

19 Riferibile, invece, alle operazioni di bonifico (cfr. *Rapporto Banca d'Italia 2026*, § 1.1): il che si spiega, naturalmente, in ragione della circostanza che «i bonifici sono impiegati prevalentemente per pagamenti, anche di importo elevato, tra persone fisiche (P2P) e tra imprese (B2B)», mentre «le carte di pagamento e la moneta elettronica, utilizzate soprattutto per l'acquisto di beni e servizi presso punti vendita fisici o virtuali (P2B), danno luogo a un numero elevato di transazioni ma di importo mediamente più contenuto» (*Rapporto Banca d'Italia 2026*, p. 5).

20 «In termini di frequenza, il numero più elevato di operazioni fraudolente riguarda ... le carte di pagamento (debito e credito), che rappresentano lo strumento più utilizzato per i pagamenti presso i punti vendita fisici e virtuali (oltre il 60% del totale delle operazioni)»: *Rapporto Banca d'Italia 2026*, p. 5.

21 Questi i dati forniti dal *Rapporto Banca d'Italia 2026*, dal quale (p. 19) sono anche tratti i periodi tra virgolette nel testo.

4. Le tipologie prevalenti di frode

Le modalità attraverso le quali vengono consumate le principali ipotesi di frodi nei pagamenti elettronici sono ormai analiticamente classificate, e può essere utile, rapidamente, ricordarne le manifestazioni principali: la più classica delle quali – ma anche, ormai, la meno insidiosa, perché più facilmente riconoscibile (e, non per caso, guardata con sempre minore indulgenza verso il cliente anche da parte dei Collegi ABF) – è sicuramente quella c.d. del *phishing*, tecnica attraverso la quale gli ignoti malfattori, sollecitando risposta a comunicazioni telematiche (per lo più, a mezzo di posta elettronica) recanti messaggi “esca”, intimidazioni allarmistiche, circostanze artefatte, etc. – e che rinviano a *link* (spesso anche assai improbabili) da cliccare o suggeriscono azioni da porre in essere – carpiscono le credenziali di accesso dell’ingenuo cliente, al fine di effettuare, a suo carico, operazioni *on line* fraudolente²². Varianti della frode appena indicata sono, com’è noto, quelle dello *smishing* e del *vishing*, nelle quali la frode si consuma attraverso, rispettivamente, l’impiego di messaggi sms o istruzioni telefoniche di finti operatori degli intermediari di riferimento del cliente ingannato (e spesso, peraltro, queste tecniche si combinano tra di loro)²³.

Con tecnica fraudolenta ben più sofisticata, altre volte, poi, i malfattori riescono finanche ad alterare la provenienza apparente della comunicazione decettiva, inserendosi nella serie dei messaggi e delle comunicazioni autentiche dell’intermediario e collocando il messaggio esca all’interno della *chat* genuina da esso intrattenuta con il cliente; o facendo apparire sul *display* del telefono del cliente un numero chiamante riconducibile all’intermediario (in tal modo riuscendo a far credere che il messaggio o la chiamata provengano effettivamente dalla banca o da un interlocutore affidabile: è il caso del c.d. *spoofing*, nelle sue diverse varianti²⁴). Le tecniche frodatorie – com’è ben noto agli operatori del settore – si sono affinate, peraltro, elaborando altre situazioni ancora più insidiose (seppure, e proprio per questo, considerate con più rigorosa attenzione ai profili di corresponsabilità degli intermediari): da quella del c.d. *boxing*, nella quale il truffatore, dopo aver intercettato la corrispondenza bancaria (posta ordinaria) inviata ai clienti, sottrae le nuove carte di credito o debito spedite per posta prima che arrivino

22 In proposito v., per tutti, P. CALDARONE, *Il phishing bancario: principali strumenti di difesa e profili di responsabilità*, in *Riv. it. inform. e diritto*, 2023, 241 ss.; G. FAILLACI, *Il phishing bancario, la responsabilità dell’ente creditizio e i suoi limiti*, in *Camm. Diritto*, 2021, 1 ss.

23 Cfr. P. PERRI, *Lo smishing e il vishing, ovvero quando l’unico limite all’utilizzo criminale delle nuove tecnologie è la fantasia*, in *Dir. dell’Internet*, 2008, 265 ss.

24 Situazioni che i Collegi territoriali ABF valutano, ordinariamente, come frodi particolarmente insidiose, tali da poter anche escludere, solitamente, la colpa grave del cliente (per tutti v. G. LEMME, *Servizi di pagamento e tutela delle persone vulnerabili*, cit., 18): peraltro, se nelle fattispecie di *spoofing* non è generalmente ravvisabile la colpa grave del ricorrente, potrà essere però ravvisato un concorso di colpa tra le parti, in relazione, da un lato, alla negligenza grave dell’utente (in particolare, ad es., in presenza di indizi di inattendibilità o anomalie del messaggio, anche in ragione della sua formulazione sintattica e grammaticale), che agevola il compimento della truffa (similmente, sotto questo profilo, a quanto avviene negli episodi di *phishing*); e, dall’altro lato, alle criticità organizzative del servizio di pagamento offerto dall’intermediario.

a destinazione, al contempo riuscendo anche a carpire al cliente, con artifici e raggiri, le credenziali di accesso²⁵; a quella (che coinvolge anche possibili profili di coinvolgimento e responsabilità degli operatori di telefonia mobile) nota come *SIM swap* (o *SIM swapping*), fattispecie fraudolenta nella quale i malfattori, dopo aver ottenuto i dati personali della vittima, inducono l'operatore telefonico a trasferire il numero su una nuova SIM, duplicata, in loro possesso: per questa via, creando una nuova corrispondenza univoca tra l'identità digitale dell'utente (in questo caso il suo numero di telefono) e la sua identità fisica (in questo caso la scheda SIM), riescono a intercettare SMS e codici OTP, usandoli per accedere ai conti bancari delle ignare vittime²⁶.

E non mancano altre esperienze fraudolente ancora più sofisticate, come ad es. quelle note come *"man in the browser"* e *"man in the middle"*: la prima, caratterizzata dall'uso di un *malware* che infetta il *browser* del *computer* della vittima, consentendo di alterare le operazioni bancarie senza che l'utente se ne accorga; mentre la seconda consiste in un attacco "in mezzo" alla comunicazione (in questo caso, l'*hacker* si interpone tra due interlocutori, fingendosi l'uno con l'altro, riuscendo così a intercettare – o addirittura modificare – i messaggi scambiati, potendo quindi operare a danno del cliente)²⁷; e l'e-

25 Secondo un consolidato orientamento dei Collegi, in caso di truffa realizzata con il contestuale utilizzo delle tecniche del c.d. *social engineering* e del c.d. *boxing*, è possibile ravvisare un concorso di colpa; tuttavia, secondo orientamento altrettanto consolidato, la colpa del cliente potrà rilevare solo nel caso in cui l'operazione contestata sia stata autorizzata previa autenticazione forte, mentre, con riguardo alla posizione dell'intermediario va anche considerato che, ai sensi dell'art. 8, comma 2, D.lgs 11/2020 "i rischi derivanti dalla spedizione di uno strumento di pagamento o delle relative credenziali di sicurezza personalizzate sono a carico del prestatore di servizi di pagamento".

26 In proposito v. R. A. HALMANN, *SIM Swapping Attacks for Digital Identity Theft: A threat to financial services and beyond*, in <https://blog.catlabs.io/>, 4 dicembre 2023; S.M. AWALE-P. GUPTA, *Awareness of Sim Swap Attack*, in *Intern. Journal of Trend in Scientific Research and Development*, 2019, 995 ss; A. GENOVESE, *L'utilizzo fraudolento degli strumenti di pagamento*, cit., 670 s., il quale sottolinea che l'orientamento dei Collegi ABF è nel senso che la truffa perpetrata con il metodo della *SIM swap fraud* comporta, normalmente, l'esclusione della colpa grave, posto che detta truffa risulta particolarmente sofisticata.

27 In sintesi, con accenni alle differenze tecniche, v. L. VARRIALE, *Man in the Middle vs Man in the Browser: le differenze che salvano il conto*, in <https://www.matricedigitale.it/>, 15 dicembre 2025. Per un caso pratico, v. M. RISPOLI FARINA, *Responsabilità degli intermediari bancari e finanziari e sistemi di internet banking: aggressione informatica e protezione del cliente*, in *Innovaz. e dir.*, 2014, 178 ss.

lenco potrebbe ancora continuare²⁸.

5. L'assetto normativo e gli obblighi delle parti

Naturalmente, a fronte di un così variegato catalogo (qui rappresentato solo parzialmente) di manovre fraudolente, la normativa di settore ha dovuto necessariamente introdurre misure idonee a contrastare il rischio di frodi e, comunque, a regolare la ripartizione delle conseguenze economiche tra intermediari e clienti²⁹; dopo una prima Direttiva in materia, del 2007, un secondo e più recente intervento europeo (direttiva n. 2366/2015) ha posto le basi della disciplina oggi vigente, quale soprattutto recata dal D. Lgs. 27 gennaio 2010, n. 11, come modificato dal D.lgs. 15 dicembre 2017, n. 218: disciplina che sarà presto innovata, peraltro, da una terza direttiva sul tema, ispirata a regole sempre più stringenti, in tema di controlli e sicurezza dei pagamenti digitali; oltre che – il che rappresenta una novità in materia – da un *Regolamento* in tema di servizi di pagamento (recante anche disposizioni già oggetto, tematicamente, della Psd2)³⁰.

Secondo la normativa oggi vigente³¹ – integrata da norme tecniche di regolamentazione dettate dall'Autorità Bancaria Europea – ogni volta che viene effettuato un pagamento attraverso strumenti digitali occorre attivare una *procedura di autenticazione*, la quale consente al prestatore dei servizi di pagamento di verificare l'identità dell'utente o la validità dell'uso di uno specifico strumento di pagamento, incluse le relative credenziali di sicurezza personalizzate fornite dal prestatore. Nelle operazioni a potenziale rischio

28 La "fantasia" dei criminali digitali, invero, elabora sempre nuove tipologie di attacchi, variamente articolati, ora sfruttando, ad es., meccanismi fisici (come, ad es., nel caso del c.d. *card trapping*, in cui la carta viene fisicamente trattenuta nel *bancomat* da un dispositivo manomesso, per essere successivamente recuperata dal truffatore), magari accompagnati dall'utilizzo di programmi insidiosi (come, ad es., nelle tecniche di *skimming*, attraverso le quali i *bancomat* o i terminali di pagamento vengono manomessi in modo da acquisire e copiare i dati dalla banda magnetica: o in quelle di truffa c.d. "*contactless*", che avviene quando un malintenzionato avvicina un terminale di pagamento portatile alle tasche o alle borse di una persona, con l'obiettivo di effettuare un micro-addebito rapido (di solito sotto i 50 euro), sfruttando la tecnologia NFC, così da non dover inserire il PIN); ora, e forse anche più frequentemente, debolezze psicologiche o comportamentali della vittima (è il caso, ad es., della truffa del c.d. "finto parente", una frode, sempre più diffusa, che vede il truffatore contattare la vittima (solitamente, persone anziane) – attraverso sms o messaggistica istantanea – da un numero (non proprio) di cellulare, facendole credere di essere un parente (il nipote, un figlio) che ha smarrito il telefono e che ha bisogno urgente di denaro, dando istruzioni per l'esecuzione di bonifici o accrediti); o, comunque, la sua collaborazione inconsapevole (come nei casi di "*card relay attack*", nei quali la carta originale rimane in possesso del legittimo titolare e il truffatore utilizza, per autenticarsi, un "clone digitale" della stessa, realizzato (attraverso la colpevole, ancorché inconsapevole "collaborazione" della vittima) mediante comunicazione NFC tra la carta e un dispositivo in possesso effettivo del truffatore, attivata a mezzo di app malevola colpevolmente installata dal ricorrente sul proprio telefono, su sollecitazione malevola del truffatore).

29 V., al riguardo, G. LEMME, *Servizi di pagamento e tutela delle persone vulnerabili*, cit., 16 ss.

30 V. *supra*, nota 7.

31 Per tutti v., in proposito, A. GENOVESE, *L'utilizzo fraudolento degli strumenti di pagamento*, cit., 658 ss.

frode (come i pagamenti elettronici a iniziativa del cliente e altre operazioni sui conti *on line*, tranne alcune eccezioni variamente giustificate) occorre una particolare procedura di autenticazione, c.d. forte, nota nel gergo di settore come SCA (acronimo che sta per *Strong Customer Authentication*, cioè autenticazione forte del cliente), la cui mancata adozione – quando essa fosse dovuta – determina senz'altro la responsabilità dell'intermediario, a cui carico è la prova³² dell'avvenuto rispetto della procedura autenticativa³³.

L'intermediario, peraltro, è tenuto anche alla osservanza di altri obblighi di comportamento, dal rispetto delle condizioni di operatività del servizio pattuite (ad es., non consentendo operazioni che superino il *plafond* concordato) all'obbligo di predisposizione di un servizio di sms *alert* (o assimilabili), attraverso il quale, una volta verificatasi una

32 Come evidenzia A. GENOVESE, *L'utilizzo fraudolento degli strumenti di pagamento*, cit., 660, «nella prassi, che registra ciò che normalmente accade nelle aule delle corti o in occasione delle procedure arbitrali presso l'ABF, la banca è solita cercare di provare l'autenticazione forte dell'operazione contestata mediante la produzione in atti delle tracciate informatiche della stessa (ad es. con i dati dei relativi log), una volta rese leggibili e trasparenti mediante la produzione in atti di un'idonea legenda». In tema v., altresì, M. RISPOLI FARINA, *Responsabilità degli intermediari bancari e finanziari e sistemi di internet banking: aggressione informatica e protezione del cliente*, cit., 172 ss.

33 Si tratta, com'è noto, di una procedura di sicurezza multifattoriale, che comporta l'utilizzo, da parte dell'intermediario, di due o più fattori di autenticazione, da combinare insieme; e precisamente:

- un elemento di conoscenza, cioè qualcosa che solo l'utente conosce, come, ad es., un PIN, una *password*, e simili altri;

- un elemento di possesso, cioè, qualcosa che solo l'utente possiede, come un *token*, una chiavetta, uno *smartphone*, e simili;

- infine, un elemento di inerenza, cioè qualcosa che solo l'utente è, che contrassegna, cioè, la persona dell'utente (come, ad es. sue caratteristiche biometriche, quali una impronta digitale, le caratteristiche fisionomiche del volto, la scansione della retina, etc.). E si richiede che l'intermediario utilizzi, nella singola operazione, almeno due dei fattori indicati (ad es., una credenziale e un OTP; una app e un dato biometrico, etc.), che devono essere tra loro indipendenti, nel senso che l'eventuale violazione di uno di essi non sia in grado di compromettere l'affidabilità degli altri.

Quando l'utente di servizi di pagamento neghi di aver autorizzato un'operazione di pagamento (che è stata) eseguita, l'utilizzo di uno strumento di pagamento registrato dal prestatore di servizi di pagamento non è di per sé necessariamente sufficiente a dimostrare che l'operazione sia stata autorizzata dall'utilizzatore medesimo, né che questi abbia agito in modo fraudolento o non abbia adempiuto con dolo o colpa grave a uno o più degli obblighi di cui all'articolo 7 D. lgs. n. 11/2010. Piuttosto, sarà onere del prestatore di servizi di pagamento fornire la prova della frode, del dolo o della colpa grave dell'utente; in mancanza di ciò, egli sarà tenuto responsabile dei pregiudizi subiti dall'utente, in ragione del rischio d'impresa sopportato: ne consegue che l'intermediario non si libera dalla responsabilità provando la mera regolarità formale delle transazioni, dovendo lo stesso, ai sensi dell'art. 10 del D. lgs. n. 11/2010, documentare elementi di fatto che caratterizzano le modalità esecutive dell'operazione dai quali possa trarsi la prova, anche in via presuntiva, della colpa grave (o del dolo) dell'utente (cfr., in particolare, Coll. Coordinam. ABF, n. 22745 del 10 ottobre 2019).

operazione sospetta, l'utente sia messo in grado di qualificare il pagamento registrato come non autorizzato³⁴; e ancora, all'adempimento di obblighi di monitoraggio delle operazioni che, tenendo conto degli aspetti che caratterizzano il normale comportamento dell'utente, consentano di rilevare operazioni di pagamento non autorizzate o fraudolente³⁵.

Naturalmente, dal canto suo, anche il cliente ha alcuni obblighi di comportamento, essendo tenuto, in particolare, a prestare diligenza nella custodia delle credenziali identificative per l'accesso ai conti e dispositive per l'esecuzione delle operazioni di pagamento; nonché alla verifica delle transazioni effettuate a valere sul proprio conto, dovendo comunicare tempestivamente all'intermediario eventuali irregolarità nella prestazione del servizio.

6. Responsabilità e rimborsi: gli orientamenti ABF

Ci si deve chiedere, a questo punto, cosa succeda – e come siano da ripartire i rischi della relativa vicenda – quando abbia avuto luogo qualche operazione dispositiva fraudolenta (tenendo conto, comunque, che, secondo la normativa vigente (D. Lgs. 11/2010) l'utente ha al massimo 13 mesi di tempo per far valere la sua pretesa al rimborso).

³⁴ Al riguardo, l'intermediario può essere esonerato solo dimostrando l'esplicito rifiuto dell'utente ad avvalersene; mentre gli effetti della mancata adozione del servizio di *alert* dovranno essere valutati alla stregua delle circostanze di fatto del caso concreto. I Collegi territoriali ABF ritengono, comunemente, che la mancata attivazione del servizio di sms *alert* (o altro assimilabile, come notifica tramite app dell'intermediario oppure *e-mail*, con una valutazione di equivalenza da condurre caso per caso) costituisca, in genere, un profilo (assorbente) di responsabilità dell'intermediario, salvo l'esplicito rifiuto dell'utente ad avvalersene (e salvo che si tratti di operazione unica, o – per le operazioni successive alla prima – di operazioni plurime poste in essere a così ravvicinata distanza di tempo l'una dall'altra (meno di cinque minuti, secondo una soluzione comunemente condivisa) da non consentire, utilmente, interventi idonei ad impedire la consumazione delle ulteriori condotte fraudolente, oltre la prima).

³⁵ In merito, la legge n. 166/2005 e il relativo decreto ministeriale di attuazione, n. 112/2007, hanno istituito un sistema di prevenzioni delle frodi sulle carte di pagamento, individuando specifici indici di anomalia di operazioni di pagamento "sospette" (in base al numero di operazioni nelle 24 ore su una stessa carta, anche tenendo conto del loro importo e della provenienza delle richieste di autorizzazione). Tale sistema si fonda, tra l'altro, sulla contribuzione, in un archivio informatizzato, dei dati identificativi delle transazioni per le quali sussiste un rischio di frode, normativamente definito nei termini di cui all'art. 8 del d.m. n. 112/2007 (si tratta, in particolare, tra le altre, delle operazioni rispondenti alle seguenti caratteristiche: tre o più richieste di autorizzazione sulla stessa carta, effettuate nelle 24 ore, presso un medesimo punto vendita (art. 8, comma 1, lett. a, n. 2); sette o più richieste di autorizzazione nelle 24 ore per una stessa carta di pagamento: art. 8, comma 2, lett. b), n. 1).

A tal proposito, secondo l'orientamento condiviso dai Collegi territoriali, le previsioni sopra richiamate non hanno un valore precettivo diretto sulla materia in esame, ma rappresentano utili indicatori per identificare anomalie e scenari di frode, anche ai sensi dell'art. 2 del Regolamento EBA n. 2018/389, in base al quale gli intermediari sono tenuti a predisporre meccanismi in grado di rilevare le operazioni di pagamento non autorizzate o fraudolente. Conseguentemente, qualora venga accertata la colpa grave del cliente, se sussistono i richiamati indici di (possibilità di) frode, i Collegi territoriali sono soliti ripartire la responsabilità con il PSP, sulla base di una valutazione caso per caso, in base agli elementi di fatto emergenti dal ricorso.

In proposito, come agevolmente si intuisce, la protezione del cliente è assicurata, anzitutto, dall'obbligo di assoggettamento delle operazioni contestate alla procedura di SCA³⁶, la quale viene richiesta (come da parere dell'Autorità Bancaria Europea del 21 giugno 2019) non solo, ovviamente, con riguardo alle singole transazioni, ma anche nella fase di *enrollment* di nuovi dispositivi, modifiche del numero certificato, installazione di app o altre operazioni similari.

Al di là di casi particolari, la procedura di SCA è generalmente richiesta; e in linea generale, molto schematicamente, si può dire che – secondo il dato normativo e l'orientamento assolutamente costante dell'Arbitro Bancario Finanziario – tutte le volte in cui fosse necessaria la procedura di autenticazione forte (SCA) e l'intermediario non l'abbia posta in essere (o, comunque, non riesca a dimostrare di averlo fatto³⁷), la sua responsabilità sarà senz'altro sussistente (con diritto del cliente al rimborso, salvo che venga provata la sua frode).

Quando, invece, sia stata dimostrata la sussistenza della SCA – sempre secondo il costante orientamento dei Collegi ABF³⁸ – la responsabilità dell'intermediario non è per ciò solo esclusa; egli, infatti, si libera da responsabilità solo se fornisce la prova del dolo o della colpa grave dell'utente, per inadempimento degli obblighi ad esso facenti capo. Colpa grave che può derivare da diverse condotte del cliente:

– ad es., per avere mal custodito le credenziali di accesso (situazione che, nei casi non infrequenti di furto o smarrimento di carte di pagamento viene spesso desunta, pre-

36 Peraltro, per alcune particolari categorie di operazioni non è richiesta tale procedura (e ciò può esporre a truffe assai insidiose), come, ad es., in un caso recentemente deciso (non favorevolmente per il cliente) da Coll. coordinamento ABF n. 8671/2024: è l'ipotesi del trasferimento di fondi da e verso conti intestati allo stesso titolare presso il medesimo intermediario (nella specie, il truffatore aveva maliziosamente carpito le credenziali di accesso della cliente, disponendo trasferimenti "inter.ni" da un conto all'altro della stessa, e inducendo poi l'ignara cliente a "restituire" l'accredito ricevuto (che le veniva rappresentato come un accredito erroneo, ma, in realtà, proveniente da altro suo conto) all'ipotetico terzo beneficiario (che era, invece, il truffatore).

37 In pratica, «qualora, a fronte del disconoscimento manifestato dall'utente, l'intermediario finanziario non sia in condizione di assolvere il suddetto onere probatorio, vale a dire qualora non riesca a dimostrare in maniera convincente che la "paternità" dell'operazione contestata sia da ricondurre all'utente stesso, egli sarà tenuto a restituire a quest'ultimo l'intera somma di cui il medesimo afferma di non aver disposto per via telematica. Grava altresì sull'intermediario, ove ne venga fatta esplicita richiesta, l'ulteriore onere di fornire la prova dell'assenza di qualsivoglia malfunzionamento nei propri sistemi informatici» (E. LUCCHINI GUASTALLA, *Strumenti di pagamento e rimedi*, cit., 91).

38 Sul ruolo e sugli orientamenti dell'ABF v., per tutti, G. Conte (a cura di), *Arbitro Bancario e Finanziario*, Milano, ed. Giuffrè, 2021; M. MAUGERI, *Il ruolo del Collegio di coordinamento all'interno del sistema ABF*, in *Riv. dir. comm. e dir. gen. obbl.*, 2024, 303 ss. L'apporto degli orientamenti arbitrali è generalmente assai apprezzato e gode di un tasso di attuazione spontanea, da parte degli intermediari, significativamente elevato (per una posizione critica, v., tuttavia, E. RECCIA, *La tipicità delle più recenti tipologie di frodi informatiche: necessità di un ripensamento? Un focus sull'attività bancaria*, in *Arch. pen.* 2022, 20 ss.).

suntivamente, dai Collegi ABF, dalla circostanza che immediatamente dopo il furto o lo smarrimento vi siano utilizzi della carta senza tentativi erronei di digitazione del PIN, così che si debba ragionevolmente dedurre che esso era improvvidamente conservato insieme alla carta);

- per avere fatto affidamento su messaggi civetta facilmente individuabili come tali (perché, ad es., recanti evidenti errori sintattici o grammaticali, manifesta non riferibilità all'intermediario, e simili);

- per aver ingenuamente seguito *link* o messaggi manifestamente sospetti, etc.

Peraltro, anche in presenza di colpa grave del cliente, potrebbe concorrere una responsabilità dell'intermediario, in ragione della violazione, da parte sua, di altri obblighi specifici ad esso facenti comunque capo:

- ad es., tipicamente, la mancata predisposizione o la mancata attuazione del servizio di *alert*, almeno tutte le volte in cui esso avrebbe potuto rivelarsi efficace (efficacia che, del tutto ragionevolmente, i Collegi ABF escludono in caso di operazione unica o di operazione/i successiva/e a brevissimo intervallo temporale dalla prima);

- oppure, l'inefficiente monitoraggio o la sussistenza di indici di anomalia idonei a segnalare operazioni sospette, etc.; nel qual caso, secondo le circostanze, potrà essere, più frequentemente, dichiarato un concorso di colpa dell'intermediario e dell'utente, con conseguente limitazione della responsabilità dell'intermediario.

L'assetto della ripartizione delle responsabilità appena richiamato³⁹ presuppone, comunque, l'esistenza di una operazione non autorizzata *disconoscibile* dal cliente (in quanto fraudolentemente posta in essere dal truffatore, *hacker*, etc.). Può accadere invece – e si tratta di situazione assai insidiosa – che il cliente, pur rimanendo vittima di un inganno posto in essere da un malfattore esterno, abbia direttamente e personalmente compiuto le operazioni, ad es., in quanto vittima di *vishing* (cioè, adescamento telefonico), seguendo pedissequamente le istruzioni che gli vengono date dal finto operatore (il che, moltissime volte risulta dalle circostanze della stessa denuncia presentata dal cliente, con valore sostanzialmente confessorio): nel qual caso (almeno allo stato della normativa oggi vigente), non sussiste una operazione di pagamento "disconoscibile" dal cliente, il quale, perciò, ne sopporterà le conseguenze; e la concorrente responsabilità dell'intermediario potrebbe configurarsi solo, secondo il diritto comune, qualora emer-

39 Rileva E. LUCCHINI GUASTALLA, *Strumenti di pagamento e rimedi*, cit., 94, che, in effetti, «quella in esame non costituisce propriamente una ripartizione di responsabilità tra le parti del rapporto, bensì configura una ripartizione del rischio connesso all'utilizzo degli strumenti di pagamento elettronici, il che rappresenta una distinzione concettuale di notevole rilevanza. In altri termini, il legislatore dell'Unione europea, nell'intento di incentivare e promuovere la diffusione dell'utilizzo degli strumenti elettronici di pagamento, ha deliberatamente scelto di porre un rischio sensibilmente più elevato a carico degli intermediari finanziari, limitando correlativamente il rischio gravante sugli utenti. Tale allocazione del rischio subisce un'eccezione, com'è naturale, nelle ipotesi in cui ricorra il dolo ovvero la colpa grave dell'utente medesimo».

gesse un suo apporto causale alla frode⁴⁰.

7. Considerazioni conclusive e prospettive evolutive

Rimangono ancora, dunque, alcune aree di rischio significative a carico dell'utente del servizio, il quale deve essere avveduto e consapevole delle molteplici e pur insidiose modalità di truffa realizzabili a suo danno, perché solo un atteggiamento prudente e accorto nell'utilizzo degli strumenti digitali di pagamento può evitare spiacevoli conseguenze pregiudizievoli.

Peraltro, a fronte di un panorama dei pagamenti elettronici che ha vissuto una profonda trasformazione, tanto nella diffusione e nelle modalità operative che nella esposizione ad attacchi malevoli (i quali rischiano di costituire una vera e propria insidia per la fiducia collettiva nel sistema digitale dei pagamenti), il pacchetto di riforme elaborato in sede UE – articolato nella nuova direttiva sui servizi di pagamento (PSD3) e nel parallelo regolamento sui servizi di pagamento (PSR), ormai in via di definitiva adozione⁴¹ – segna un cambio di paradigma fondamentale nel contrasto ai crimini informatici in ambito finanziario, imponendo l'adozione di misure di sicurezza assai più stringenti di quelle

40 In tal caso, «la fattispecie...non è sussumibile nell'ambito del citato d. lgs.» (in tal senso, ex multis, Coll. ABF Palermo, decisione n. 2090 del 4.2.2022; Coll. Palermo, decisione n. 10042 del 04.06.2020; Coll. Roma, decisione n. 4658/21 del 22.02.2021; Coll. Roma, 4962 del 23.3.2022). Invero, in ragione della diretta riconducibilità al cliente dell'operazione posta in essere, dovrà allora valere la considerazione secondo la quale «per quanto la volontà del cliente di effettuare [l'operazione] sia stata viziata per effetto del raggio subito dal terzo ignoto, l'intermediario non poteva che considerare autorizzata» l'operazione effettuata «personalmente dal titolare», con la conseguenza di non poter considerare non autorizzata l'operazione compiuta «personalmente dal ricorrente, sia pure sulla base del vizio di volontà sopra descritto» (in tal senso, testualmente, Coll. ABF Milano, n. 8602/2021). In casi del genere, una concorrente responsabilità del PSP potrebbe astrattamente venire in rilievo, secondo le norme di diritto comune, solo qualora emergesse dalla documentazione in atti un apporto causale dell'intermediario alla frode come, ad esempio, nei casi di:

- mancata disponibilità (anche temporanea) del numero verde del PSP, che impedisca all'utente di accertare in via preliminare la genuinità delle indicazioni fornite dal frodatore;
- mancata identificazione del tentativo di frode in corso da parte del dipendente del PSP, al quale il pagatore si sia rivolto esponendo le richieste del frodatore;
- mancato rilievo di indici di frode nel caso in cui il cliente sia stato indotto dal frodatore a disporre dei pagamenti nella convinzione di effettuare degli accrediti in conto e il blocco delle transazioni lo avrebbe reso consapevole dell'effettiva natura delle operazioni poste in essere.

In proposito v., ad es., A. GENOVESE, *L'utilizzo fraudolento degli strumenti di pagamento*, cit., 662 s.

41 La cui pubblicazione nella G.U.C.E. è attesa, ormai, per la fine del 2026, con termine a circa metà 2028 per la sistemazione a regime.

attuali⁴² e delineando un regime di rimborsabilità rafforzato a favore degli utenti ingannati da sofisticati attacchi malevoli, come, in particolare, in caso di *spoofing*.

E questo spostamento dell'asse di responsabilità, che trasferisce l'onere economico dal cliente finale – spesso l'anello debole della catena – agli operatori finanziari e alle piattaforme informatiche, costringerà certamente l'intera filiera tecnologica a investire in algoritmi di intelligenza artificiale di nuova generazione per l'analisi predittiva del rischio transazionale e il blocco tempestivo delle anomalie. È naturale, peraltro, che l'efficacia del nuovo quadro normativo nel contenimento delle frodi dipenderà, realisticamente, dall'equilibrio che il mercato saprà trovare tra rigore di sicurezza e fluidità dell'esperienza utente. La sicurezza digitale non può risolversi in un'architettura punitiva o inutilmente complessa per il cittadino, ma deve configurarsi come un processo impercettibile e predittivo, capace di proteggere la transazione senza penalizzare, però, la competitività del commercio elettronico; la sfida che si apre per i prossimi anni, conseguentemente, non è soltanto tecnica, ma prevalentemente culturale: l'integrazione tra la disciplina europea, lo sviluppo di tecnologie difensive avanzate e la costante alfabetizzazione digitale degli utenti rappresenterà, probabilmente, l'unico vero scudo in grado di proteggere l'economia digitale del prossimo futuro.

42 Dalla estensione sistematica del controllo di corrispondenza tra il nome del beneficiario e il codice IBAN/identificativo di pagamento per i bonifici (al fine di azzerare i rischi di impersonificazione e truffe via ingegneria sociale), all'introduzione di assetti normativi tali da consentire la condivisione tempestiva di indicatori di frode ed elementi comportamentali tra istituti di credito, nel rispetto delle norme sulla protezione dei dati personali (GDPR); ma, soprattutto, con l'adattamento dei requisiti di autenticazione per rispondere ai nuovi scenari di consumo (es. pagamenti in app o tramite intelligenza artificiale), introducendo modalità alternative per garantire l'inclusione delle fasce di utenza più vulnerabili.