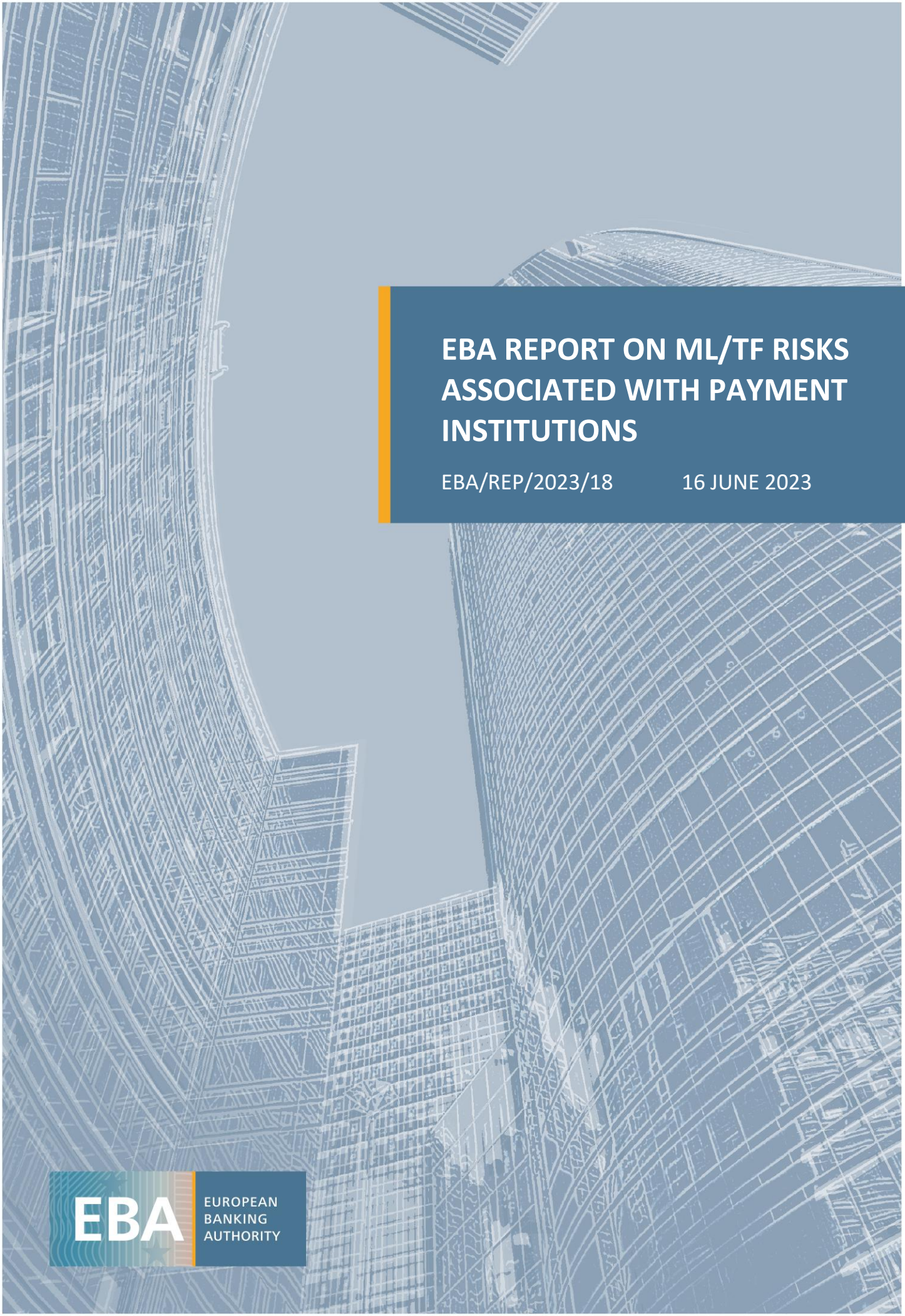


EBA REPORT ON ML/TF RISKS ASSOCIATED WITH PAYMENT INSTITUTIONS

EBA/REP/2023/18 16 JUNE 2023

EBA EUROPEAN BANKING AUTHORITY

Contents

List of abbreviations

AISP	Account information service provider
AMLD	Anti-Money Laundering Directive (Directive (EU) 2015/849)
AML	Anti-money laundering
CASP	Crypto asset service provider
CDD	Customer due diligence
CFT	Countering the financing of terrorism
EBA	European Banking Authority
FIU	Financial Intelligence Unit
MS	Member States
NRA	National risk assessment
PEP	Politically exposed person
PI	Payment institution
PSD2	Payment Services Directive (Directive (EU) 2015/2366)
SNRA	Supranational risk assessment
TF	Terrorist financing

Executive summary

Payment institutions are subject to Directive (EU) 2015/849 ('AMLD') for anti-money laundering and terrorist financing (AML/CFT) purposes. Therefore, they should have in place systems and controls to identify, assess, monitor and manage money laundering and terrorist financing (ML/TF) risks. At the same time, in line with the risk-based approach, AML/CFT supervisors should adjust the frequency and intensity of their supervisory activity to monitor effectively, and to take measures as necessary, to ensure compliance of payment institutions with the AMLD.

In 2022, the EBA carried out an assessment of ML/TF risks in the payment institutions sector. The objective of this risk assessment was to better understand:

1. the scale and nature of the ML/TF risk associated with the payment institutions sector;
2. the extent to which payment institutions' AML/CFT systems and controls are adequate and effective in tackling those risks; and
3. the extent to which current supervisory approaches to tackling ML/TF risk in payment institutions are effective.

The EBA's findings suggest that ML/TF risks in the payment institutions sector may not be assessed and managed effectively. In particular, the EBA found the following:

- AML/CFT supervisors across Europe consider that payment institutions, as a sector, represent high inherent ML/TF risks. At the same time, the systems and controls payment institutions put in place to mitigate those risks are not always effective.

- Not all AML/CFT supervisors base the frequency and intensity of on-site and off-site supervision on the ML/TF risk profile of individual payment institutions, and on the ML/TF risks in that sector.

- Supervisory practices at authorisation vary significantly, and AML/CFT components are not consistently assessed. As a result, payment institutions with weak AML/CFT controls operate in the EU and may establish themselves in MS where the authorisation process is perceived as less stringent to passport their activities cross-border afterwards.

- There is no EU-level common approach to the AML/CFT supervision of agent networks, or the AML/CFT supervision of payment institutions with widespread agent networks. The use of agents by payment institutions carries a significant inherent ML/TF risk, especially in a cross-border context.

Addressing these points will be essential to protecting the EU's single market from financial crime. It will also help improve access by payment institutions to payment accounts by addressing a root cause of de-risking.

Findings of this risk assessment will feed into the EBA's bi-annual ML/TF risk assessment exercise. Some risks, such as virtual IBANs or white labelling, have recently emerged and need further assessment by the EBA. Others require changes to the EU legal framework, such as: establishing a more consistent approach to assessing the AML/CFT component of the authorisation of payment

institutions; reinforcing the consideration of ML/TF risks in the process of passporting notifications and ultimately establishing clear and coherently interpreted provisions for objection, on ML/TF risk grounds, in the passporting context; or taking steps towards a more consistent treatment, by MS, of agents of payment institutions in a cross-border context, including a more coherent approach to the AML/CFT supervision of such agents across Europe.

1. Background

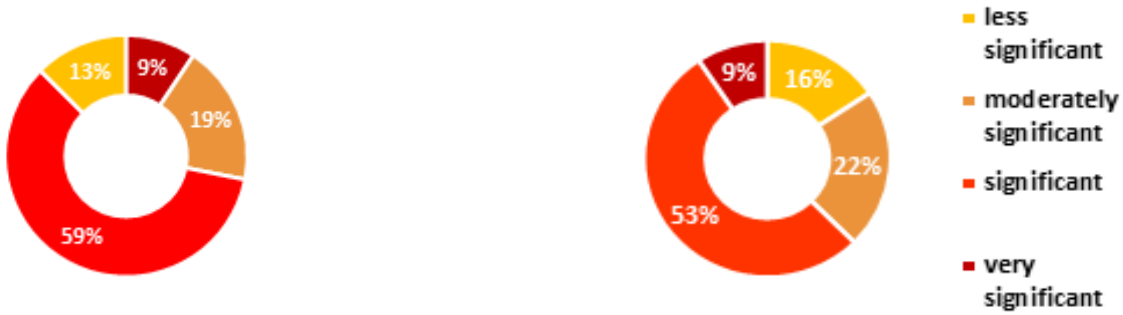
Payment institutions are commonly associated with higher ML/TF risks. For example:

- The EBA, in its 2021 Opinion on ML/TF risk factors affecting the European Union's financial sector[1], noted that more than two-thirds of all AML/CFT supervisors considered that the sector poses significant or very significant ML/TF risks. It also noted that the significant risk profile associated with this sector did not always appear to be matched with a commensurate level of supervisory activity in all cases.

- The European Commission, in its 2022 supranational risk assessment[2], considered that payment institutions are inherently exposed to both ML and TF risks and they 'appeared to be most vulnerable to risks arising from weaknesses in AML/CFT systems and controls'.

- Payment institutions are impacted, as customers, by de-risking. 'De-risking' refers to decisions taken by financial institutions to refuse to onboard or to discontinue servicing existing customers that they associate with higher ML/TF risks.

Figure 1: Overall level of inherent risk (first chart) and residual risk (second chart) of the payment institutions sector, as perceived by European AML/CFT supervisors, 2022.



This raises concerns about:

- the robustness of the overall implementation, by payment institutions, of AML/CFT measures; and
- the adequacy and proportionality of the level of resources allocated by national competent authorities to the AML/CFT supervision of the payment institutions sector.

[1] Issued in March 2021 and accessible here: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf

[2] Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities {SWD(2022) 344 final}, published on 27 October 2022, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554

In April 2022, the EBA decided to assess:

- the scale and nature of ML/TF risk associated with the sector;
- the extent to which payment institutions' AML/CFT systems and controls are adequate and effective in tackling those risks; and
- the extent to which current supervisory approaches to tackling ML/TF risk in payment institutions are effective.

The EBA carried out this assessment on the basis of Article 9a(5) of the EBA founding regulation.

1.1. Methodology

Article 9a(5) of Regulation (EU) 1095/2010[3] mandates the EBA to 'perform risk assessments of the strategies, capacities and resources of competent authorities to address the most important emerging risks related to money laundering and terrorist financing at Union level as identified in the supranational risk assessment'.

Such risk assessments are a fact-finding tool to assess and support the ability of all competent authorities or a cross-section of competent authorities to address specific, strategic, emerging ML/TF risks. Emerging risks include new risks that have not been identified before, and existing risks that have significantly increased or taken on a new significance.

In carrying out these risk assessments, the methodology requires the EBA to draw on information available to it. Accordingly, the information sources used for the risk assessment of payment institutions included[4]:

- responses by 32 European AML/CFT supervisors to an EBA survey on ML/TF risks associated with payment institutions, carried out in 2022;
- the Commission's supranational risk assessments and staff working documents;
- the EBA's PSD2 peer review on the authorisation of payment institutions;
- the EBA's Opinions on ML/TF risks affecting the EU financial system;
- MS national risk assessments, as well as competent authorities' sectoral risk assessments of the payment institutions sector, where available;
- bilateral exchanges with selected national competent authorities responsible for the AML/CFT supervision of payment institutions in the context of this risk assessment;
- other available work on ML/TF risks in payment institutions from reputable sources, including the FATF and the Council of Europe.

1.2. Applicable legal framework and scope of the risk assessment

Payment institutions are obliged entities under Directive (EU) 2015/849[5] (AMLD). This means that they are subject to the same AML/CFT requirements as other financial institutions in the EU. Where

[3] EBA founding regulation of 24 November 2010, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02010R1093-20210626&qid=1677573282068&from=en

[4] Please see the full list of sources in the Annex.

[5] Directive (EU) 2015/849 of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015L0849&from=EN

applicable, activities by payment institutions as payment service providers are also governed by Regulation (EU) 2015/847[6] (the Transfer of Funds Regulation, TFR).

Payment services are further regulated by Directive (EU) 2015/2366[7] (the Payment Services Directive, PSD2), which in its Annex lists a range of services, including:

- services enabling cash to be placed on or withdrawn from a payment account;
- execution of payment transactions such as direct debits or credit transfers;
- execution of payment transactions through payment cards or similar devices;
- issuance of payment instruments and/or acquiring of payment transactions;
- money remittance;
- payment initiation services;
- account information services.

This risk assessment focusses on payment institutions that are authorised to provide payment services in the EU. It does not assess the risks associated with unregistered, or unauthorised, payment institutions.

[6] Regulation (EU) 2015/847 of the European Parliament and of the Council of 20 May 2015 on information accompanying transfers of funds

[7] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance); OJ L 337, 23.12.2015, p. 35-127

2. ML/TF risks identified in the payment institutions sector

The high inherent risk associated with payment institutions is based on the following risk factors[8]:

1. the customer base;
2. the cash-intensive nature of the services offered;
3. the prevalence of occasional transactions rather than established business relationships;
4. the high-risk jurisdictions in which or with which PIs operate;
5. the large overall volume and high speed of transactions across the sector;
6. the use of new technologies to facilitate the onboarding of customers remotely; and
7. the distribution channel used (especially the network of intermediaries incl. agents).

Not all payment institutions are exposed to the same level of ML/TF risk. This is because the sector is not homogeneous. Instead, it encompasses entities with a variety of sizes and business models. Different business models will affect the extent to which each payment institution is exposed to ML/TF risk.

For example, AML/CFT supervisors consider ML/TF risks to be particularly increased for payment institutions that provide cash-based money remittance services and that do not enter into a business relationship with their customer that would trigger the application of customer due diligence (CDD) measures. By contrast, they perceive the inherent ML/TF risks linked to the activities of account information service providers (AISPs) to be limited, as AISPs are not involved in the payment chain and do not hold customer funds.

At the same time, most AML/CFT supervisors assess payment institutions' AML/CFT controls as insufficient to mitigate those risks effectively. Some AML/CFT supervisors indicated to the EBA that, following their supervisory engagement, institutions' AML/CFT controls have slightly improved compared to previous years, but this has not translated into improved overall residual risk ratings yet.

The EBA notes that some MS, in their national risk assessments, assess the level of residual risk in the PIs sector as moderate or medium. This is because they consider that the impact of high inherent ML/TF risks and poor controls in this sector is limited because PIs hold bank accounts and that any transactions channelled through those accounts are subject to banks' own internal AML/CFT control measures.

2.1. Risks linked to customers of payment institutions

According to EU AML/CFT supervisors, based on information from regulatory returns and supervisory findings, payment institutions tend to have a customer base with a high proportion of potentially higher-risk customers:

[8] Sources: the Commission's staff working document accompanying the supranational risk assessment of 27 October 2022, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN and the successive Opinions of the EBA on the risks of money laundering and terrorist financing affecting the European Union's financial sector, EBA/Op/2021/04 of 3 March 2021, JC2019 59 of 4 October 2019 and JC/2017/07 of 20 February 2017

- For individual customers this may include non-residents, or individual customers who have been de-risked from the banking sector. Two AML/CFT supervisors reported an increased PEP presence in the customer base of their PIs sector.

- For institutional customers, the number of customers from certain high-risk sectors – including gambling companies and crypto asset service providers (CASPs) – is proportionately higher than in the banking sector. New client typologies are also emerging, such as platforms and marketplaces, which, by creating additional layers, seem to increase the overall ML/TF risk level.

AML/CFT supervisors from MS where the PIs sector focuses on servicing local customers indicated that the overall ML/TF risks are lower than in MS where the sector has a cross-border outlook. Some AML/CFT supervisors reported that they were making efforts to re-focus PIs' business models on the local market, with mixed results. A general perception of AML/CFT supervisors is that payment institutions tend to have a higher risk appetite than, for instance, retail banks.

2.2. Geographical risks linked to payment institutions

AML/CFT supervisors consider that geographical risks are major risk factors in this sector and linked to both, ML and TF concerns. Three AML/CFT supervisors indicated to the EBA that the most significant risk associated with payment institutions in their MS is the cross-border nature of transactions executed by the sector, often with high-risk third countries. Another seven AML/CFT supervisors indicated that transactions from or to high-risk third countries constituted the second most significant ML/TF risk factor linked to PIs in their MS. One AML/CFT supervisor specifically referred to 'off-shore countries' as an additional element.

AML/CFT supervisors consider that geographical risk is particularly prevalent in PIs that are **money remitters**. Money remitters oftentimes operate in geographical areas where credit institutions are less present and where they legitimately provide access to payment services filling the gap of absent credit institutions. AML/CFT supervisors reported that there is a high number of transfers by money remitters to third countries that are associated with higher levels of ML/TF risk; however, the overall volume of these transactions remains limited.

2.3. Risks linked to the types of products and services offered by payment institutions

Risks linked to the product/service offered by PIs depend on individual institutions' business models. General risk factors mentioned by AML/CFT supervisors include products and services allowing anonymity through new technologies, the use of innovative products, the high speed of transactions, the use of cash and the one-off type transactions without an associated payment account.

Most NRAs flagged that the use of **new technologies** and the provision of new types of services by payment institutions carries higher ML/TF risk. This statement is also confirmed by responses of AML/CFT supervisors to the EBA. The higher ML/TF risk is linked to new technologies and remote customer onboarding, trades with crypto assets and the use of AI solutions for both individual risk scoring and transaction monitoring purposes, which remain ill understood.

The use of **cash** is also a risk factor. All AML/CFT supervisors considered that the higher ML/TF risks stem from those business models which allow the sending of cash from the payer to the payee without an established business relationship of either of the two counterparties. In some MS, where the use of cash in the economy is generally declining, the money remittances sector remains the most efficient way of sending cash abroad, and the process is usually more affordable and quicker than it would be through the banking sector. While the number of operations remains high, the average value of the cash being

sent remains low or moderate. It is worth mentioning that there is the trend in several MS that, instead of physical cash handover, the customer transfers money to the money remitter by PayPal or other transfer (excl. funds transfer from a bank), thereby adding an additional transaction to the chain of cash remittance.

AML/CFT supervisors agreed that the prevalence of occasional or **one-off transactions** is a risk factor. Many transactions executed by the payment institutions are of an occasional nature, which means that the institution will not establish a stable relationship with the customer. What is more, in many MS occasional transactions are exempt from the application of CDD measures. Consequently, the ability of payment institutions to create a customer risk profile and to identify and manage ML/TF risks associated with individual transactions is limited.

2.4. Risks linked to delivery channels and the use of intermediaries (agents)

AML/CFT supervisors indicated in their responses to the EBA's survey on ML/TF risks associated with payment institutions that the prevalence of non-face-to-face business relationships without adequate risk management tools may increase the level of ML/TF risk exposure of the payment institutions sector.

Nevertheless, AML/CFT supervisors concur that the most significant risk associated with PIs' delivery channels is the widespread use of **intermediaries, including agents**. The economic advantage of using a network of intermediaries is to achieve the widest possible reach to customers, including in areas where access to financial services, including money transfer services, is otherwise limited.

The business models of agents can vary. Members States' NRAs suggest that the agents' core business is not always linked to the financial services industry, and that instead agents are newsagents, internet and phone stores, tobacco shops, mini markets and petrol stations. This can limit agents' awareness of applicable AML/CFT rules and consequently the effective application of AML/CFT controls put in place by appointing payment institutions. Evidence also suggests that many agents serve one or more payment institutions at the same time and that agents frequently change payment institutions. This can make oversight by payment institutions of their agent network difficult and create significant AML/CFT systems and controls weaknesses. This is because agents are not normally obliged entities themselves and because the ultimate responsibility for compliance with AML/CFT requirements remains with the appointing PI. Information provided to the EBA by AML/CFT supervisors suggests that this risk has crystallised and that consequently the risk that agents are being exploited by criminals or criminal networks is high.

2.5. Risks emanating from outsourcing of AML/CFT-related tasks of PIs

AML/CFT supervisors consider that the risk related to outsourcing by payment institutions of important AML/CFT functions to third parties is high.

Outsourcing can help institutions to access specialised services and to achieve better compliance outcomes, often at a competitive cost. However, without appropriate safeguards it can adversely affect the robustness of institutions' control and risk management framework. For example, it may undermine the overall competencies and independence of the outsourcing PI.

Furthermore, outsourcing in a cross-border context can jeopardise the PI's 'local substance', which is required by PSD2[9]. 'Local substance' refers to the need for payment institutions to have their head office in the MS where they are seeking authorisation and to conduct part of their activities there so that PIs are effectively managed and controlled in the jurisdiction in which they obtained authorisation. The

[9] Art 11(3) of Directive (EU) 2015/2366 (PSD2)

EBA's 2023 peer review on authorisation under PSD2[10] revealed significant differences across MS regarding the interpretation of this provision. Failure to ensure local substance means the lack of close links with the jurisdiction where the payment institution is established. When the payment institution is not effectively managed and controlled in the jurisdiction where it was established, it can contribute to a limited oversight of the quality of the outsourced service.

2.6. Other risk factors: Brexit

The 2019 and 2021 EBA Opinions on ML/TF risk highlighted risks arising for the EU's financial sector from the withdrawal of the UK from the EU. This risk was related to the relocation of institutions, previously headquartered in the UK, to EU MS. The relocation of PIs hitherto authorised in the UK, which was accompanied by an increased number of authorisation requests within a limited timeframe, posed AML/CFT challenges.

AML/CFT supervisors from some MS confirmed that PIs that had relocated to their MS posed risks linked to inadequate AML/CFT systems and controls and a poor compliance culture. For example, AML/CFT systems and controls requirements imposed upon them at authorisation (e.g. reinforcement of their compliance functions, recruitment of local staff, etc.) had not yet been implemented and created significant ML/TF vulnerabilities. The impact of this risk materialising was increased as some payment institutions were growing at an accelerated pace post-authorisation, and passported their services throughout the EU.

2.7. Emerging risks in the PIs sector

Competent authorities identified three emerging risks in the sector. These related to 'white labelling', virtual IBANs and third-party acquirers.

Several AML/CFT supervisors highlighted that '**white labelling**' was a rising trend and was of ML/TF concern. White labelling means that payment institutions make their licence available to independent agents which develop their own product under the licence of the regulated financial institution. In its response to the call for advice on the revision of PSD2[11], the EBA highlighted that agents acting under the license of white label can have control over the business and over the business relationship, including the communication with payment service users. They may also come into possession of funds and obtain control of the financial flow. This can lead to an increase in ML/TF risk exposure which the payment institution may be ill-equipped to manage.

AML/CFT supervisors also highlighted the issuance and use of virtual International Bank Account Numbers (**virtual IBANs**) by payment institutions as an emerging risk. Virtual IBANs look identical to IBAN codes but do not have the capacity to hold any actual balance; they are only used to reroute incoming payments to a regular IBAN linked to a physical bank account. The use of virtual IBANs creates ML/TF risk because they obfuscate the geography where the underlying account is located and this risks creating gaps in supervisory coverage. It can also mean that payment institutions do not comply with the applicable AML/CFT framework.

[10] EBA report on the peer review on authorisation under PSD2, EBA/REP/2023/01 of 11 January 2023, available here: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1050744/Peer%20Review%20Report%20on%20authorisation%20under%20PSD2.pdf

[11] Opinion of the EBA on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), EBA/Op/2022/06 of 23 June, available here: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

Third-party merchant acquiring has been identified as an emerging trend, and potentially a new ML/TF risk. In this setting, the merchant acquirer (which is the entity providing payment processing services to merchants incl. authorisation, clearing or settlement) outsources certain parts of the acquiring process to a third-party acquirer (TPA), TPAs are oftentimes obliged entities themselves. TPAs then perform services for the merchant on the acquirer's behalf and are responsible for complying with the AML/CFT laws of the respective jurisdiction (within or outside the EU) when onboarding and monitoring the merchant. This exposes the acquirer to the risk of indirectly processing illicit funds through the TPA in the event that the TPA's AML/CFT programme is vulnerable to ML/TF and/or sanctions violations. TPA transactions cause a segmentation of the acquiring business resulting in an increased ML/FT risk, including transaction-based laundering, or risk of other fraudulent activities.

3. Implementation of AML/CFT measures by payment institutions

There is a general perception amongst EU AML/CFT supervisors that the payment institutions sector's implementation of AML/CFT measures is less robust than, for example, that of the banking sector. ML/TF risk awareness of the sector is perceived to be limited.

3.1. AML/CFT weaknesses identified

The Commission's staff working document, published alongside the 2022 SNRA, indicates that AML/CFT supervisors consider that payment institutions are less aware of money laundering risks than the banking sector, for example. Their internal AML/CFT control systems are also perceived as insufficient.

This is in line with findings from the EBA's biennial ML/TF risk assessment exercise. AML/CFT supervisors' responses suggest that controls are often inadequate to manage the ML/TF risk to which institutions in this sector are exposed. The most common weaknesses identified by AML/CFT supervisors include:

- **A poor overall awareness of ML/TF risk**. While the quality of business-wide and individual RAs in the sector has improved slightly in the last three years, it remains a significant concern. Some AML/CFT supervisors pointed to the lack of rigorous training on AML/CFT issues, especially where agents are used.

- **Insufficient transaction monitoring.** Most AML/CFT supervisors indicated that failure to monitor transactions in a meaningful way is pervasive in the sector, with transaction monitoring systems deficient or not in place at all.

- **Insufficient suspicious transaction identification and reporting (STR)**. Lack of awareness of ML/TF risk and deficiencies in ongoing transaction monitoring contribute to the sector's limited ability to identify unusual transactions and to report suspicious transactions. AML/CFT supervisors assessed the adequacy and effectiveness of STR reporting as poor or very poor. AML/CFT supervisors reported that many PIs appear to rely on the STR reporting systems of the credit institutions with which they bank, rather than implement their own as would be required under the applicable EU legal framework.

- **Failure to implement systems and controls to comply with restrictive measures.** AML/CFT supervisors indicated poor or insufficient implementation, and a limited understanding, by the sector, of restrictive measures regimes. Specific issues identified were linked to the ongoing screening of customers and transactions, which in some institutions was happening sporadically or not at all.

- **Weak internal governance arrangements**. Some AML/CFT supervisors found that the payment institutions sector under their supervision had inadequate internal governance arrangements. This was the case especially where payment institutions were new entrants seeking rapid growth and maximum profit. Findings included the lack of application of a clear three-lines-of-defence system as well as a relatively high turnover of staff in the key function holder positions. One AML/CFT supervisor pointed out the active participation of shareholders in the running of the business, which could interfere with the institution's sound and prudent ML/TF risk

management. These elements may collectively contribute to weakening the payment institutions' wider governance arrangements, including their risk management frameworks.

- **TF risks are poorly understood and managed.** In line with the Commission's staff working document of 2022, many AML/CFT supervisors considered that terrorist financing risk associated with payment institutions is significant. This risk is linked to specific features of the product and services on offer, such as the cash-based nature and the wide geographical reach of the service, which usually involves low-value transactions. It is also linked to a more limited understanding, by the sector of TF risks, and reliance on sanctions screening as the only TF risk mitigating tool.

- **Remote/online onboarding without appropriate safeguards**. AML/CFT supervisors referred to specific weaknesses stemming from the remote onboarding of customers in the sector, without appropriate safeguards. As part of this, AML/CFT supervisors noted that payment institutions often failed to identify high-risk customers, including PEPs.

3.2. AML/CFT breaches by PIs

As part of the EBA's survey on ML/TF risks associated with payment institutions, AML/CFT supervisors indicated that most breaches in the sector related to ongoing monitoring, internal controls and overall AML/CFT policies and procedures, customer identification and verification of ID, and customer and business-wide risk assessment. This is broadly in line with the quality of controls that competent authorities were generally concerned about in the sector.

The same deficiencies are mirrored by AML/CFT supervisors' submissions to the EBA's AML/CFT database, EuReCA, which was put in place in January 2022 as part of the EBA's renewed AML/CFT mandate. European supervisors are required to report identified AML/CFT-related weaknesses in entities under their supervision, including payment institutions. The sector of payment institutions is the second most reported sector to EuReCA, after credit institutions. Since EuReCA's establishment in January 2022, competent authorities have reported 62 material weaknesses in relation to 19 payment institutions[12], out of which 59 were 'breaches' or 'potential breaches'. One PI had their licence withdrawn during that period on AML/CFT grounds.

Figure 2: Most common breaches identified in the payment institutions sector, 2022

[12] Data extracted from EuReCA as of 5 May 2023

4. Supervision of the PIs sector

In July 2017, the EBA issued guidelines which specify which documentation applicants should submit for the purpose of authorisation as a payment institution across MS[13]. The documentation requested includes, among other things, information on the applicant's internal AML/CFT systems and controls[14].

AML/CFT internal controls include a business-wide ML/TF risk assessment, AML/CFT policies and procedures including oversight of agent networks, and a governance structure where responsibility for AML/CFT compliance is clearly allocated.

European supervisors responsible for the authorisation of payment institutions are therefore expected to scrutinise the documentation in order to satisfy themselves that:

- the applicant's ML/TF risk assessment is appropriate and complete;
- the applicant has or will put in place adequate systems and controls to ensure that the ML/TF risks associated with its branches, agents or distributors are managed effectively;
- the person designated as responsible for the PI's compliance with AML/CFT requirements has sufficient AML/CFT expertise to carry out their functions.

Once authorised, the payment institution should be supervised effectively for AML/CFT compliance. To achieve this, the EBA's guidelines on risk-based supervision provide that AML/CFT supervisors identify and assess the ML/TF risks associated with the payment institution, both individually (i.e. entity-level risk assessment) and as a sector (i.e. sectoral risk assessment). These risk assessments, conducted on a regular basis, should form the basis of AML/CFT supervisors' supervisory strategy, including the nature and extent of their supervisory activity and their approach to enforcement. European supervisors in charge of AML/CFT supervision should also constructively interact with their prudential counterparts and other stakeholders at the national level and internationally to ensure a targeted, comprehensive and consistent supervisory approach based on the best information available.

The EBA found that not all supervisors are doing enough to manage ML/TF risks in the sector effectively.

4.1. Authorisation/licensing of payment institutions

In 2022, the EBA reviewed the implementation of its authorisation guidelines through an EBA peer review[15]**.** Based on the findings from this peer review and related information from the EBA's ongoing work on AML/CFT, the EBA is of the view that some of the weaknesses identified in section 3.1 that relate to the adequacy of PIs' internal AML/CFT controls are linked to current authorisation practices. Specifically, the peer review findings suggest that in some MS authorisation processes are not as robust as they should be, which means that applicants are able to obtain a licence in spite of inadequate AML/CFT controls.

[13] EBA Guidelines under Directive (EU) 2015/2366 (PSD2) on the information to be provided for the authorisation of payment institutions and e-money institutions and for the registration of account information service providers, GL/2017/09 of 11/07/2017 available here: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1904583/f0e94433-f59b-4c24-9cec-2d6a2277b62c/Final%20Guidelines%20on%20Authorisations%20of%20Payment%20Institutions%20%28EBA-GL-2017-09%29.pdf?retry=1

[14] Based on Article 33 of PSD2, AISPs are exempted from providing information on their internal AML/CFT controls and systems upon their registration.

[15] EBA/REP/2023/01 of 11 January 2023, available here: Peer Review Report on authorisation under PSD2.pdf (europa.eu)

In particular, the EBA observed the following:

1. Most supervisors in charge of the authorisation process under PSD2 collected the requisite information on the applicant's internal AML/CFT controls in line with the EBA GLs on authorisations[16], but the degree of scrutiny of the respective documents varies across competent authorities, and in some cases this information is not assessed at all. Obtaining information, including documents, without assessing them is not sufficient to be satisfied that the applicant has the necessary AML/CFT internal control mechanism in place.

In some cases, the EBA found evidence that an assessment was carried out, but without the involvement of experts with the necessary AML/CFT expertise. In other cases, AML experts were involved in the assessments, but their expert opinion was not adequately considered in the final decision on authorisation.

2. Not all supervisors that are responsible for the authorisation of payment institutions have criteria or a methodology against which they would assess the applicant's business-wide ML/TF risk assessment. In the absence of such criteria, or a robust methodology, the competent authority may not be able to:
    - provide its own objective assessment as to whether the applicant's entity-wide RA is adequate and complete to ensure that the applicant PI understands its ML/TF risks;
    - identify inconsistencies, or inadequate or unrealistic identification or assessment of the risks by the applicant;
    - assess the applications in a consistent, uniform and systematic way, independently of the actual staff member completing the assessment;
    - provide meaningful feedback to the applicant as to whether their assessment was appropriate.

The ML/TF risk assessment is central to the applicant's AML/CFT-related documentation in particular because the adequacy of the applicant's AML/CFT controls and systems and mitigating measures will be assessed on the basis of the ML/TF risk assessment. The lack of a clear and objective methodology on the part of the competent authority for the scrutiny of the applicant's ML/TF risk assessment may lead to acceptance of applicants with inadequate understanding of their ML/TF risk exposure.

3. Not all AML/CFT supervisors verify the background of the person in charge of the applicant's AML/CFT compliance in a risk-sensitive way. The peer review revealed significant differences in supervisors' practices across MS, with some supervisors reporting that they do not assess the suitability and expertise of the person in charge of implementing the applicant's AML/CFT obligations as part of the authorisation process at all, as this is not required by their national law. Other competent authorities reported that they conduct some analysis on the background and expertise of the applicant, however practices vary significantly across MS.

[16] EBA Guidelines on the information to be provided for the authorisation of payment institutions and for the registration of account information service providers under Article 5(5) of Directive (EU) 2015/2366, EBA/GL/2017/09 of 11 July 2017, available here: BoS 2017 XX Final Report on Guidelines on Authorisations.docx (europa.eu)

In the absence of a thorough assessment, it is not possible to determine if the person in charge of the applicant's AML/CFT compliance is suitable and competent[17]. The adverse consequences of authorising a payment institution with unsatisfactory results for the suitability of the person who will then be responsible for designing and implementing the PI's internal AML/CFT framework can be significant. If, in addition, this is coupled with inadequate ML/TF risk assessment and associated AML/CFT controls, the management of the PI is unlikely to be prudent, safe and sound.

4.2. AML/CFT supervisors' risk assessment on the PIs sector

The EBA, in its guidelines on risk-based supervision, provides that supervisors should assess the ML/TF risk associated with the sectors under their supervision. They should also assess risk at the level of individual institutions, or groups of institutions ('subjects of assessment') subject to certain conditions. MS national risk assessment can go some way towards meeting these expectations.

All MS but one shared with the EBA their **national risk assessment**, which took different formats and contained different levels of detail. Some NRAs were outdated (i.e. published in 2017-2018 based on earlier data), others were currently under revision by the national authorities. The EBA found that the NRA was usually insufficient for AML/CFT supervisors to achieve a good understanding of the ML/TF risks of the PIs sector under their supervision.

As part of the EBA's survey on ML/TF risks associated with payment institutions, a large proportion of AML/CFT supervisors indicated that the data they provided for their assessment of the ML/TF risks and of the quality of controls in the payment institutions sector was based on a formal risk assessment as envisaged in the EBA's guidelines on risk-based supervision. However, only a small proportion of AML/CFT supervisors provided that formal **sectoral ML/TF risk assessment** to the EBA upon its request. This suggests that the basis for the AML/CFT supervisors' risk assessment of the PIs sector is instead stemming from the NRA, or from a general view of inspection findings without an underlying risk assessment methodology. These findings align with findings from the EBA's reviews of AML/CFT supervisors' approaches to tackling ML/TF risk in the banking sector, where the lack of a robust sectoral risk assessment methodology is a recurring observation[18].

As for the **entity-level ML/TF risk assessment**, AML/CFT supervisors confirmed that these are usually based on an annual self-assessment questionnaire, sent to PIs under their direct supervision. Given that the payment institutions sector is very heterogeneous (i.e. size, business model, national vs. foreign), AML/CFT supervisors indicated that they found it difficult to design a questionnaire that was suitable for all types of payment institutions, but most had not taken steps to adjust their questionnaire to take account of those differences. Some AML/CFT supervisors also highlighted that the quality of information obtained from the sector can be very different depending on the type and maturity of the respondent institutions. They also said that some institutions did not submit the requested data at all.

In some cases, the information collected from individual PIs is adjusted based on other information to which the AML/CFT supervisor has access, including in some cases information from the FIU or relevant

[17] On 14 June 2022, the EBA published guidelines on the role of AML/CFT compliance officers, EBA/GL/2022/05, which specify the role, tasks and responsibilities of the AML/CFT compliance officers. These guidelines are applicable to payment institutions and are available here: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2022/EBA-GL-2022-05%20GLs%20on%20AML%20compliance%20officers/1035126/Guidelines%20on%20AMLCFT%20compliance%20officers.pdf

[18] EBA report on competent authorities' approaches to AML/CFT supervision of banks (Round 2, 2020/2021), EBA/REP/2022/08 available here: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2022/1028593/Report%20on%20CAs%20approaches%20to%20AML%20CFT%20supervision.pdf

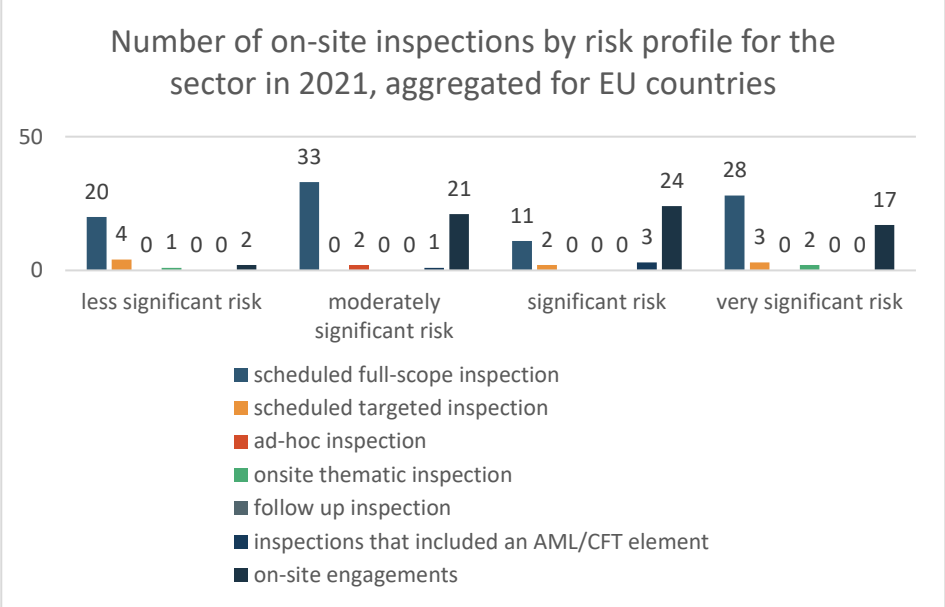
enforcement agencies. In the context of the Article 9a(5) risk assessment, the EBA could not obtain sufficient information to conclude if the entity-level risk assessment of the payment institutions is conducted in an appropriate way in all MS.

4.3. Allocation of supervisory resources for the payment institutions sector's supervision

The majority of AML/CFT supervisors have one supervisory team in charge of AML/CFT supervision of all financial sectors, including PIs, but some AML/CFT supervisors indicated that they had established dedicated teams specifically for the AML/CFT supervision of payment institutions. Where no separate teams were in place, AML/CFT supervisors confirmed that they needed to make trade-offs, in their everyday supervisory work, to decide as to whether they use their scarce resources for supervision of payment institutions or of institutions in other sectors instead.

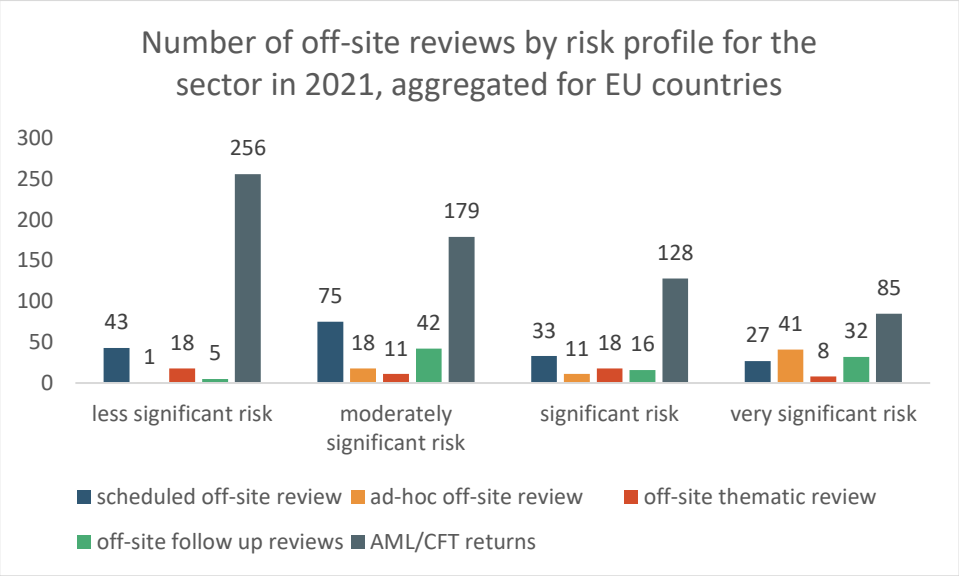
Responses to the EBA's survey on ML/TF risks associated with payment institutions suggest that AML/CFT supervisory activities in relation to payment institutions are less frequent than in the banking sector; and that the proportion of on-site or off-site inspections[19] in payment institutions falls below that of credit institutions, which are also assessed as carrying increased ML/TF risk. This raises concerns about the adequacy of AML/CFT supervision of this sector. It also raises concerns about the adequacy of supervisory risk assessments, because, in the absence of adequate supervisory activities, AML/CFT supervisors may not have the necessary information available in order reliably to feed it into their risk assessment of the entities and of the whole sector.

Figure 3: Aggregated number of on-site inspections in payment institutions, by risk profile of the institutions, 2021



[19] While the definition of 'on-site inspection' and 'off-site review' may vary across MS, for the Article 9a(5) risk assessment the definitions applied are those taken from the EBA's risk-based supervision guidelines (EBA/GL/2021/16 of 16 December 2021).

Figure 4: Aggregated number of off-site reviews in payment institutions, by risk profile of the institutions, 2021



AML/CFT supervisors indicated that on-site inspections, which can be intrusive and comprehensive, and therefore resource-intensive, usually concentrate on the payment institutions which represent the highest ML/TF risks. However, data received in the context of the EBA's survey on ML/TF risks associated with payment institutions does not indicate that this happens consistently in practice (please refer to Figures 3 and 4). Furthermore, pursuing this strategy, whilst it is in line with a risk-based approach in principle, means that some payment institutions may remain without any intrusive supervisory activity from the AML/CFT supervisor over a significant period of time. An analysis of data reported to EuReCA suggests that most systems and controls weaknesses are identified during on-site inspections. The low number of intrusive inspections therefore suggests that the number of shortcomings may be greater in practice compared to what Figure 2 shows.

4.4. Approaches to AML/CFT supervision of intermediaries across EU MS

Articles 45(2) and 48(4) of the AMLD provide that, where a credit or financial institution operates an establishment in another MS, that establishment has to comply with the AML/CFT rules of the host MS, and will be supervised by the AML/CFT supervisor of the host MS. Agents are not obliged entities under the AMLD and are not themselves required to comply with the AML/CFT rules in the host MS in which they operate. This means that when a payment institution provides payment services through agents in another MS territory, the appointing payment institution retains the obligation to comply with the AML/CFT requirements of that MS. When a Member State extends the scope of the AMLD to agents, agents need to comply with the AMLD themselves.

As indicated in section 2.4, the use of agents is considered by almost all AML/CFT supervisors as high-risk. The EBA has previously highlighted significant differences in AML/CFT supervisors' approaches to the AML/CFT supervision of the activities carried out by agents[20]. Previous EBA work and bilateral exchanges in the context of the Article 9a(5) risk assessment confirmed that that there is no common

[20] Opinion of the EBA on the nature of passport notifications regarding agents and distributors under Directive (EU) 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive (EU) 2015/849 (AMLD), EBA-Op-2019-03 of 24 April 2019, available here: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/da05ad8a-eed2-410a-bd08-072403d086f3/EBA%20Opinion%20.pdf

supervisory practice across the EU with regard to off-site or on-site AML/CFT inspections in relation to agents, or payment institutions' AML/CFT oversight of their agent network. The ultimate risk is that this high-risk activity may remain unsupervised for AML/CFT purposes.

In the majority of the MS, agents are not obliged entities under the EU AML Directive and therefore they are not legally bound to comply with the national AML/CFT obligations of the jurisdiction in which they are carrying out their activities. Several AML/CFT supervisors confirmed to the EBA that, as host supervisors, they do not have any direct supervisory remit over these entities. Two MS opted for a different approach whereby they designated agents in their territory as obliged entities themselves. In one MS, agents are supervised by a public agency (also responsible for the registration of agents) which itself is supervised by the AML/CFT supervisor.

Payment institutions are perceived to lack appropriate control over the network of agents, especially in a cross-border context. The risk of agents being exploited by criminals or criminal networks is perceived as high. Additional identified challenges to AML/CFT supervisors related to the fact that the same agent may serve several principals, which can lead to situations whereby no principal will have a full view on the entirety of transactions of a single customer, which may use several payment institutions through the same agent.

In situations where the AML/CFT supervisor of the country where the agent is based does not have direct oversight of the agent itself but would intend to sanction the agent, such a situation would require the opening of a disciplinary proceeding against several payment institutions, as principals, for the failure to supervise the same agent. Also, some agents move frequently from one principal PI to another, and sometimes principals are even based in different countries. Such frequent changes make it difficult to implement any enforcement actions from the AML/CFT supervisor: the former principal is not in charge anymore and facts have to be established again against the new principal.

The EBA is of the view that some of the difficulties AML/CFT supervisors identified in relation to the use of agents were already visible at the stage of the authorisation process of PIs. Results of the EBA's PSD2 peer review exercise revealed that the applicant's proposed use of a network of agents is not always assessed thoroughly during the authorisation process. Some national legislation does not require the applicant to provide information on its branches, agents and distributors at all, although this is explicitly required by the EBA guidelines on authorisation of payment institutions. Also, one-third of the supervisors participating in the peer review exercise indicated that they do not have a methodology or criteria to assess the information the applicant may provide on the measures it has or will put in place to ensure AML/CFT compliance by its agents. Therefore, it remains unclear what assessment supervisors undertake with regard to the information on agents and distributors, even when such information is provided by the applicants.

4.5. AML/CFT aspects of the passporting notifications

PSD2 provides for the possibility for PIs, established in an EU MS, to use agents to offer their payment services in any other MS. Regulatory technical standards specify the method, means and details of cooperation, between the home and host supervisors, concerning the agent passport application and the information to be included therein[21]. The qualification of such agents as an establishment (or not) in the host MS is crucial to determine a certain number of reporting measures and other obligations applicable for them in the host MS. The main risk is that agents in a cross-border context would fall outside of any AML/CFT supervisory radar.

[21] Commission Delegated Regulation (EU) 2017/2055, supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for the cooperation and exchange of information between competent authorities relating to the exercise of the right of establishment and the freedom to provide services of payment institutions, issued 23 June 2017

In situations where the activities of the agents qualify as an 'establishment', additional obligations are triggered in the host MS. This includes the obligation to comply on the appointing PI's behalf with the host MS's AML/CFT requirements[22]. The host MS also then has the possibility to require the appointment of central contact points[23] (under certain conditions). Therefore, the determination of whether the agent's activity within the host MS qualifies as an establishment (or, alternatively, as free provision of services) is crucial. The EBA found that national supervisory approaches and criteria for deciding on an 'establishment' vary across MS, although the qualification as an establishment (or the free provision of services) should be included in the passporting notification. This determination is even more challenging for services provided online.

The passporting notification is provided by the home supervisor for the attention of the host supervisor, on the first occasion where the principal PI expresses its intention to provide services outside the country of its establishment. PSD2 provides that the host supervisor should alert the home supervisor of any 'reasonable grounds for concern'[24] in connection with the intended engagement of an agent with regard to ML/TF. If, subsequently, the assessment of the home NCA is not favourable, then it must refuse to register the agent, or withdraw the registration if already made.

Passporting notifications are handled by prudential supervisors, oftentimes by the licensing department which also decides on the licensing applications. During bilateral exchanges with the EBA, many AML/CFT supervisors indicated that they are not required or invited by prudential supervisors to provide their view on the passporting notifications, which will in those cases be accepted without due consideration of ML/TF risks. In addition, the EBA found that some authorities interpreted 'reasonable grounds for concern with regard to ML/TF' as amounting to a criminal conviction, rather than ML/TF risk, which makes a refusal unlikely. The EBA is aware of very few examples where passporting was refused based on 'reasonable grounds for concern' expressed at the stage of the passporting notifications.

The EBA has repeatedly called for the need to clarify, in the Level 1 text, the consistent treatment by MS of activities carried out by payment institutions through agents and intermediaries in a cross-border context. Strengthening the effective oversight of agents by their principals is of importance. Direct regulation and supervision should apply for instance when the combination of services from different principals is done in such a way that principals cannot manage risks.

4.6. Ongoing AML/CFT supervision in a cross-border context

In respect of the supervision of agents or branches of a payment institution located in another Member State, cooperation is required between the home and the host supervisors. In accordance with PSD2, where the home supervisor intends to carry out an on-site inspection of a branch or an agent of the payment institution located in another Member State, it should notify the host supervisory authority in writing. The home supervisor can also delegate the task of conducting an on-site visit to the host supervisor, in which case it needs to provide the host supervisor with reasons for requesting such an on-site inspection. Similarly, the host supervisor can request the home supervisor to carry out an inspection in the head office of the payment institution, and such a request should also be reasoned and sent in writing. Also, in situations where the payment institution, carrying out its activities in another MS, changes the passporting information communicated in its initial application, the home supervisor should transmit to the host supervisor the information affected by the changes.

[22] Articles 45(2) and 48(4) and recitals 52-53 of the AMLD
[23] Delegated Regulation (EU) 2018/1108 of 7 May 2018, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1108&rid=4
[24] Article 28(2) of PSD2

The EBA heard from AML/CFT supervisors during the bilateral exchanges that host AML/CFT supervisors may not always have real visibility on the scope of the activities carried out, at any time, in their jurisdictions other than the initial notification.

What is more, there is no common view on the treatment, for AML/CFT oversight purposes, of services that are provided online, nor is there a consistent application of requirements by the host jurisdictions. As a result, some payment institutions appear to have made use of regimes that they perceived to be more permissive to obtain authorisation and passport their services into other MS.

As indicated by several AML/CFT supervisors during the bilateral exchanges with the EBA, AML/CFT colleges remain an important forum of cooperation and information exchange across AML/CFT supervisors for PIs operating in several MS on a cross-border basis. The EBA observed a growing number of AML/CFT colleges for payment institutions in its most recent report on AML/CFT colleges[25].

[25] The EBA report on the functioning of AML/CFT colleges in 2021, EBA/REP/2022/18 of 1 September 2022, available here: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2022/1038179/Report%20on%20functionion%20of%20AML%20CFT%20Colleges.pdf

5. Conclusion and next steps

There are nearly 900 authorised PIs in the EU. The perception of AML/CFT supervisors in charge of the AML/CFT supervision of these PIs is that this sector represents a significant inherent ML/TF risk. AML/CFT supervisors also consider that the internal AML/CFT systems and controls of institutions in the PIs sector are not robust enough to mitigate these inherent ML/TF risks.

Directive (EU) 2015/849 requires AML/CFT supervisors to monitor effectively, and to take the measures necessary to ensure compliance by financial institutions with this directive. As part of this, it requires competent authorities to adjust the frequency and intensity of on-site and off-site supervision to reflect the outcomes of their ML/TF risk assessments. The EBA issued guidelines to competent authorities on the steps they should take to comply with these requirements.

In 2022, the EBA assessed the scale and nature of ML/TF risk in the sector, and the extent to which that risk is managed effectively by institutions and AML/CFT supervisors.

The EBA's findings suggest that not all competent authorities are currently doing enough to comply with their legal obligations in respect of the AML/CFT supervision of payment institutions. This means that ML/TF risks in the payment institutions sector may not be assessed and managed effectively, which may impact the integrity of the EU's financial system. The EBA's work on access to financial services suggests that failure to address those risks will also undermine efforts to improve access by payment institutions to payment accounts. Indeed, de-risking could be warranted if the risk associated with individual payment institutions is assessed as unmanageably high.

Specifically, the EBA's findings suggest the following:

- The AML/CFT internal controls in payment institutions do not seem robust enough to mitigate the ML/TF risks identified.

- Not all competent authorities base the frequency and intensity of on-site and off-site supervision on the ML/TF risk profile of individual payment institutions, and on the ML/TF risks in that sector.

- Supervisory practices at authorisation vary significantly, and AML/CFT components are not consistently assessed. As a result, payment institutions with weak AML/CFT controls can operate in the EU and may establish themselves in MS where the authorisation process is perceived as less stringent to passport their activities cross-border afterwards.

- There is no common approach to the AML/CFT supervision of agent networks, or the AML/CFT supervision of payment institutions with significant agent networks. The use of agents by payment institutions carries a significant inherent ML/TF risk, especially in a cross-border context.

Several of these findings relate to issues addressed in existing EBA guidelines, including in particular the risk factor guidelines and the guidelines for risk-based supervision. A more robust implementation by

supervisors of provisions in these guidelines will therefore go some way to mitigating those risks and reduce the sector's exposure to ML/TF risks.

Other findings require changes in the EU legal framework. They relate in particular to the establishment of a more consistent approach to assessing the AML/CFT component of the authorisation of payment institutions; and reinforcing provisions regarding the consideration of ML/TF risks in the process of passporting notifications and ultimately establishing clear and coherently interpreted provisions for objection, on ML/TF risk grounds, in the passporting context. They are also necessary to ensure a more consistent treatment, by MS, of agents of payment institutions in the cross-border context, including a more coherent approach to the AML/CFT supervision of such agents across Europe. The EBA's technical advice on the review of PSD2[26] and the EBA's peer review on authorisation under PSD2[27] contain further detail on these points.

Findings of this risk assessment, in line with Article 9a(5) of the EBA founding regulation, will be feeding into the EBA's bi-annual ML/TF risk assessment exercise. Emerging ML/TF risks, including virtual IBANs and white labelling, will need further assessment.

The EBA remains committed to tackling ML/TF risk holistically, across all financial sectors within its remit.

[26] Opinion of the EBA on its technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), EBA/Op/2022/06 of 23 June 2022, available here: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

[27] Report on the peer review on authorisation under PSD2, EBA/REP/2023/01, published on 11 January 2023 and available here: Peer Review Report on authorisation under PSD2.pdf (europa.eu)

Annex: list of sources used for the Article 9a(5) risk assessment

Applicable EBA publications:

Opinion on the ML/TF risks affecting the EU's financial sector, EBA/Op/2021/04 of 3 March 2021, available here:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2021/963685/Opinion%20on%20MLTF%20risks.pdf;

JC2019 59 of 4 October 2019, available here:
https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/1605240c-57b0-49e1-bccf-60916e28b633/Joint%20Opinion%20on%20the%20risks%20on%20ML%20and%20TF%20affecting%20the%20EU%27s%20financial%20sector.pdf

JC/2017/07 of 20 February 2017, available here:
https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1759750/cedce61c-279b-4312-98f1-a5424a1891ad/ESAS%2520Joint%2520Opinion%2520on%2520the%2520risks%2520of%2520money%2520laundering%2520and%2520terrorist%2520financing%2520affecting%2520the%2520Union%25E2%2580%2599s%2520financial%2520sector%2520%2528JC-2017-07%2529.pdf

The ML/TF risk factors guidelines, EBA/GL/2021/02 of 1 March 2021, available here:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

Guidelines on risk-based supervision, EBA/GL/2021/16 of 16 December 2021, available here:
https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2021/EBA-GL-2021-16%20GL%20on%20RBA%20to%20AML%20CFT/1025507/EBA%20Final%20Report%20on%20GL%20on%20RBA%20AML%20CFT.pdf

Guidelines on the information to be provided for the authorisation of payment institutions and for the registration of account information service providers under Article 5(5) of Directive (EU) 2015/2366, EBA/GL/2017/09 of 11 July 2017, available here:
BoS 2017 XX Final Report on Guidelines on Authorisations.docx (europa.eu)

Report on the peer review on authorisation under PSD2, EBA/REP/2023/01, published on 11 January 2023 and available here:
Peer Review Report on authorisation under PSD2.pdf (europa.eu)

Opinion on the nature of passport notifications regarding agents and distributors under Directive (EU) 2015/2366 (PSD2), Directive 2009/110/EC (EMD2) and Directive (EU) 2015/849 (AMLD), EBA-Op-2019-03 of 24 April 2019, available here:

https://www.eba.europa.eu/sites/default/documents/files/documents/10180/2622242/da05ad8a-eed2-410a-bd08-072403d086f3/EBA%20Opinion%20.pdf

RTS on the framework for cooperation and exchange of information between competent authorities for passport notifications under Directive (EU) 2015/2366, EBA/RTS/2016/08 of 14/12/2016, available here: https://www.eba.europa.eu/sites/default/documents/files/documents/10180/1694291/7a77aa22-dcc8-44a7-89ec-5779eb1c4bbc/Final%20draft%20RTS%20on%20passporting%20%28EBA-RTS-2016-08%29.pdf?retry=1

RTS on cooperation between competent authorities in home and host MS in the supervision of payment institutions on a cross-border basis under Article 29(6) of PSD2, EBA/RTS/2018/03 of 31 July 2018, available here: EBA BS 2018 XX (Draft RTS on home-host cooperation under PSD2 - Final Report).docx (europa.eu)

Report on potential impediments to the cross-border provision of banking and payment services, 29 October 2019, available here: https://www.eba.europa.eu/sites/default/documents/files/document_library/EBA%20Report%20on%20potential%20impediments%20to%20the%20cross-border%20provision%20of%20banking%20and%20payment%20services.pdf

Opinion on the technical advice on the review of Directive (EU) 2015/2366 on payment services in the internal market (PSD2), EBA/Op/2022/06 of 23 June 2022, available here: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Opinions/2022/Opinion%20od%20PSD2%20review%20%28EBA-Op-2022-06%29/1036016/EBA%27s%20response%20to%20the%20Call%20for%20advice%20on%20the%20review%20of%20PSD2.pdf

Other sources:

The Commission's supranational risk assessments and staff working documents

Report from the Commission to the EU Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, {SWD(2022) 344 final}, published on 27 October 2022, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022DC0554

The Commission staff working document ('Annex') accompanying the risk assessment, available here: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0344&from=EN

Results of the EBA survey on 32 European AML/CFT supervisors' opinions on ML/TF risks associated with payment institutions, 2022

EBA bilateral exchanges with selected national competent authorities interviewed for the Article 9a(5) risk assessment

National risk assessments of MS, as well as NCAs' sectoral risk assessments on the payment institutions sector, where available

Other available work on payment institutions (incl. FATF publications and CoE reports, including the series of CoE country reports on the assessment of the concrete implementation and effective application of the 4th AML Directive in the EU Member States)

EUROPEAN BANKING AUTHORITY

Tour Europlaza, 20 avenue André Prothin CS 30154
92927 Paris La Défense CEDEX, FRANCE

Tel. +33 1 86 52 70 00

E-mail: info@eba.europa.eu

https://eba.europa.eu