ML/TF Risks Identified in the European Payment Institution Sector

Ireland

September 2023

Introduction: Niamh Lambe

Whilst fighting financial crime has been a priority for regulators and payment institutions (PIs), both are under immense pressure to move away from 'tick-box' compliance by innovating and promoting a culture of compliance to better protect our communities. As the level of regulatory scrutiny increases, regulated PIs will need to strategically examine whether their identification and management of Money Laundering / Terrorist Financing (ML/TF) risks is effective.

On 16 June 2023, the European Banking Authority (EBA) published a report on ML/TF risks associated with EU PIs. The EBA assessed the scale and nature of ML/TF risk in the PIs sector. It considered how PIs identify and manage ML/TF risks and what supervisors do to mitigate those risks when considering an application for the authorisation of a PI and during the life of a PI.

The EBA's findings suggest that generally institutions in the sector do not identify and manage ML/TF risk adequately and internal controls in PIs are often insufficient to prevent ML/TF. This is in spite of the high inherent ML/TF risk to which the sector is exposed due to the nature of their business. Failure to manage ML/TF risks in the PIs sector can impact the integrity of the EU's financial system and may also undermine efforts to improve access by PIs to payment accounts.

KPMG recognises the significance of these observations and has compiled below a summary of the areas that the EBA Report covers in relation to ML/TF risks associated with PIs.

Niamh Lambe
Managing Director
Head of Financial Crime
KPMG in Ireland

ML/TF Risks Identified in the European Payment Institution Sector

The EBA considers the payment institution sector to represent high inherent ML/TF risks. High risk factors include the customer base, geography, type of the financial products offered and the channels used to deliver them. Some examples of risks are set out below.

01

CUSTOMER

PIs have an increased customer base of individuals who have been previously de-risked from the banking sector due to AML/CFT concerns.

The number of customers from high-risk sectors such as gambling companies and crypto asset service providers (CASPs) is higher compared with the banking sector.

02

GEOGRAPHICAL

The cross-border nature of transactions, which are often executed with high-risk third countries, represents increased risk of ML/TF.

03

PRODUCT

Products and services can facilitate anonymity, through new technologies, innovative products and the high speed of transactions.

There is a prevalence of occasional transactions rather than established business relationships, resulting in PIs being unable to create a customer risk profile to support the identification and management of ML/TF risks.

04

DELIVERY CHANNEL

There is widespread use of intermediaries, including agents who have limited awareness of applicable AML/CFT rules and for which oversight is difficult by PIs. The risk that agents are being exploited by criminals or criminal networks is high.

Outsourcing without appropriate safeguards and oversight in place can adversely affect the robustness of PIs' control and risk management frameworks.

Emerging Risks

The use of **Virtual IBANs** has been identified as the most relevant emerging risk in the sector. 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.

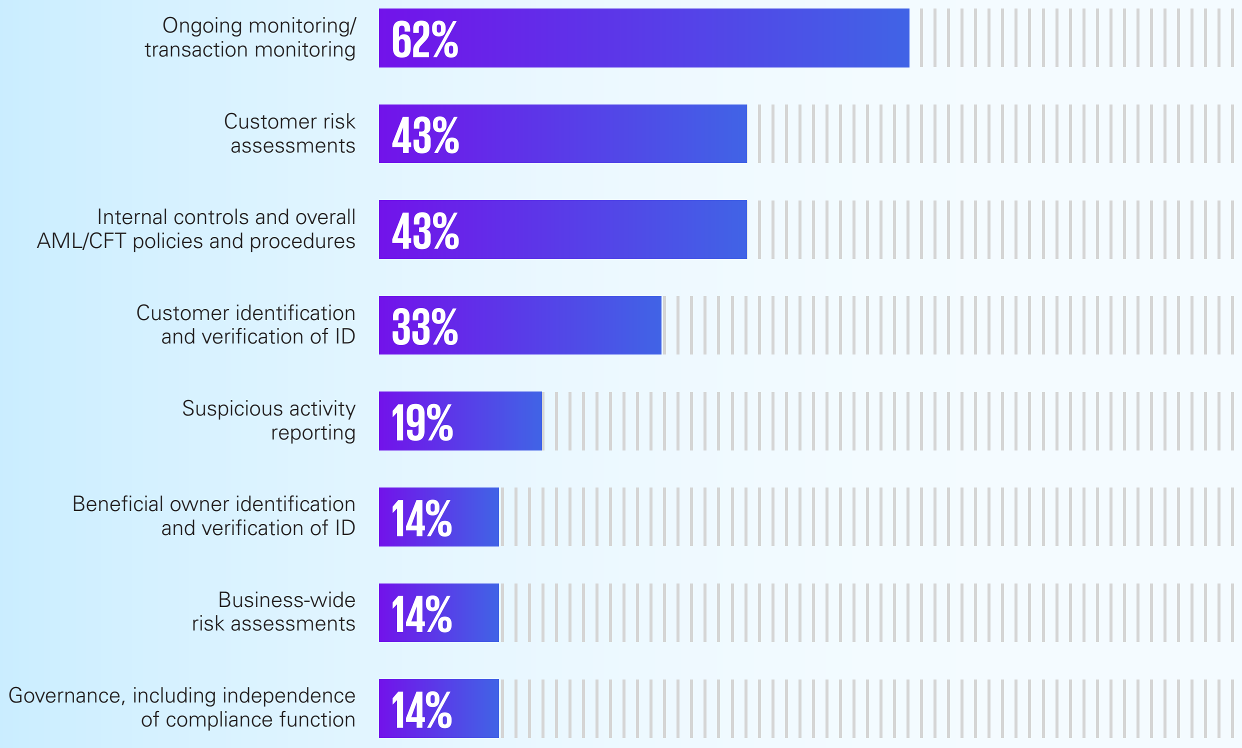
Other emerging risks identified are **White Labelling**, occurring when PIs make their licence available to independent agents which develop their own product under the licence of the regulated financial institution, or **Third-party merchant acquiring**, when the entity providing payment processing services to merchants (incl. authorisation, clearing or settlement) outsources certain parts of the acquiring process to a third-party acquirer.

ML/TF Risks Identified in the European Payment Institution Sector

Weaknesses identified

The EBA, in its report, has identified weaknesses that involve a poor overall awareness and management of ML/TF risks and lack of rigorous training on AML/CFT issues. The deficiencies in the treatment of AML/CFT has led to regulatory breaches.

The most common breaches in the treatment of AML/CFT risks by the payment institution sector for 2022 are as follows:



** Most common AML/CFT breaches identified in the payment institutions sector, 2022 (EBA REPORT ON ML/TF RISKS ASSOCIATED WITH PAYMENT INSTITUTIONS, EBA/REP/2023/18 of 16 JUNE 2023)*

The most common weakness is related to deficient transaction monitoring systems. Other weaknesses found are derived from insufficient suspicious transaction identification and reporting (STR). Many PIs appear to rely on the STR reporting systems of the credit institutions with which they bank, rather than implementing their own.

The EBA also noted for some PIs that the ongoing screening of customers and transactions was not happening on a consistent basis or was not happening at all. It was also noted that internal governance arrangements were inadequate with a lack of application of a clear three-lines-of defence approach.

Other risks identified were associated with the participation of shareholders in the running of the business, which interfered with the PI's sound and prudent ML/TF risk management.

The EBA observed that TF risks are poorly understood and managed, particularly because of the specific features of the product and services such as the cash-based nature and the wide geographical reach of the service. The EBA noted the reliance on sanctions screening as the only TF risk mitigating tool.

Conclusion and next steps

The EBA's findings suggest that PIs are inherently exposed to greater ML and TF risks compared with other sectors due to the nature of their business models. The systems and controls they put in place are not robust enough to mitigate the ML/TF risks identified. Addressing these weaknesses in the EBA report will be essential to protecting the EU and Ireland market from financial crime.

Findings of the EBA's assessment represented by the published report will feed into the EBA's bi-annual ML/TF risk assessment exercise. It is expected that the EBA will continue to strive towards 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.

How KPMG can help

We are ready to assist you in the identification and assessment of Money Laundering and Terrorism Financing risks. We can help you understand the regulatory requirements and incorporate them into your broader strategies to ensure a safe environment for your customers, which will fuel your growth in the market. KPMG has an active, market leading global financial practice, with proven methodologies and risk libraries to meet regulatory expectations. We combine this with our substantial experience in the use of tech and data to support our clients in driving the right risk, regulatory and cost outcomes.

Drawing on deep sectoral experience, we can support you in the following:

Risk Assessment Methodology

- Conducting review and assurance exercises on your Risk Assessment Methodology and your AML framework to evaluate ML/TF threats and risks to your business;
- Ensuring that all relevant risk criteria have been adequately identified and assessed against known and emerging typologies and tailored for the risks presented in your business model;
- Reviewing your risk assessments to ensure they are supported by both qualitative and quantitative data;
- Ensuring your key risk indicators are adequately identified and reported within the business;
- Designing and implementing controls to effectively mitigate these risks; and,
- Sharing global better practice insights to help shift your mindset towards transformation and innovation in the way your company treats risks, including emerging risks.

Achieving operational excellence in Transaction Monitoring

- Ensuring adequate identification of risk scenarios against the risk assessment;
- Assessment of detection scenarios to ensure sufficient coverage;
- Advising on data lineage across the customer lifecycle to ensure integrity;
- Advising on the right tools, technology, strategy, analytics and data to help you move to innovative customer and transaction monitoring; and,
- Ensuring that data usage is optimised, and tech is configured to reduce level of false positives and therefore cost.

Fincrime Operating Model

- Support you in assessing your Fincrime operating model across tech, data, people and process;
- Developing and executing a technology strategy and operating model that supports the utilisation and development of existing and future data for a more effective AML program;
- Implementing a dynamic system of Customer Identification and Verification, Customer Due Diligence and Customer Risk Assessment, including PEPs, for a more effective mitigation of Risks;
- Providing benchmark practices, including the use of tech and data and capability against peers, mindful of emerging technologies;
- Optimising investment spend, to give you best bang for your buck; and,
- Devising a roadmap and supporting implementation for the maturing of your operational model, based on the specific AML risks your company wants to address, to meet the ever-changing FinCrime landscape.

Get in touch

Ian Nelson
Partner
Head of Financial Services,
Head of Regulatory Consulting
m: +353 87 744 1989
e: ian.nelson@kpmg.ie

Niamh Lambe
Managing Director
Head of Financial Crime
m: +353 87 050 4388
e: niamh.lambe@kpmg.ie

Noleen Scullion
Director
Regulatory
m: +353 87 744 1559
e: noleen.scullion@kpmg.ie

Rachel McMahon
Director
Risk Consulting
m: +353 87 111 7961
e: rachel.mcmahon@kpmg.ie

kpmg.ie

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

If you've received this communication directly from KPMG, it is because we hold your name and company details for the purpose of keeping you informed on a range of business issues and the services we provide. If you would like us to delete this information from our records and would prefer not to receive any further updates from us please contact unsubscribe@kpmg.ie.

Produced by: KPMG's Creative Services. Publication Date: September 2023. (9449)