RocaJunyent Informs

Prevention of Money-Laundering and Terrorist Financing Department

13 December 2024

1. The state of the sector

Nearly all Fintechs are subject to AML/CTF regulations (Law 10/2010, of 28 April, on the Prevention of Money Laundering and Terrorist Financing, and its Regulation, Royal Decree 304/2014). This is because they operate as credit institutions, payment institutions, investment service companies, or providers of virtual currency exchange services for fiat currency and electronic wallet custody, among other activities. However, surprisingly, many of these Fintechs are not fully aware of their status as obliged entities or the responsibilities this entails.

Non-compliance with these obligations poses a significant issue for Fintechs, given the potential impact on their businesses. It is not just about the financial penalties stipulated by the regulations, which can amount to millions or even lead to the closure of regulated activities, but also the reputational damage that could deter shareholders, banks, suppliers, and even potential customers.

Notably, the Ministry of Economy, Trade and Business, and the Treasury Department highlighted in their Addendum to the National Risk Analysis 2024 that the use of technological innovations in financial operations is one of the top five vulnerabilities in the prevention of money laundering and terrorist financing.

AML/CTF regulations impose on obliged entities the responsibility to ensure their services are not used for money laundering or terrorist financing and to identify operations indicative of these crimes.

Current challenges: General obligations for Fintechs regarding AML/CTF

While new European regulations have been published this year, which will be discussed further, they are not yet applicable. To date, the main obligations of Fintechs can be summarised as follows:

Formal obligations:

- Risk assessment report: Maintain a risk assessment report identifying and evaluating risks across products, services, customers, geography, systems, or channels used for fund movements. This document must be reviewed periodically and updated whenever a significant change occurs that could influence the entity's risk profile.
- Internal AML/CTF manual: Document internal control procedures that must meet minimum requirements established by regulations (e.g., client admission policy, due diligence procedures, procedures for detecting transactions subject to special examination, as outlined in Article 33 of RD304/2014).
- Designated representatives: Appoint a Representative to SEPBLAC and establish an Internal Control Body responsible for implementing policies and procedures.
- Internal communication channels: Provide channels for reporting suspicious activity and breaches of national and internal AML/CTF regulations.
- Annual training plan: Approve an annual AML/CTF training plan for all staff, tailored according to each team's risk exposure.
- Document retention policies: Maintain documentation retention policies in compliance with AML/CTF regulations.
- External evaluation: Undergo annual assessment by an External Expert.

Substantive obligations

- Customer Due Diligence (CDD): Implement robust Know Your Customer (KYC) processes for accurate customer identification.

- Continuous monitoring: Monitor business relationships and operations on an ongoing basis.

- Suspicious activity detection: Identify and conduct Special Examinations of suspicious transactions.

- Operational abstention: Refrain from executing any transactions with indications of money laundering or terrorist financing.

- Non-disclosure: Adhere to non-disclosure obligations regarding potential SEPBLAC reports or operation reviews related to money laundering or terrorist financing.

- Mandatory reporting: Report suspicious transactions to SEPBLAC.

- Collaboration with authorities: Cooperate with authorities.

While these obligations require both technological and human resources, including highly specialised staff, the regulations and the regulator allow outsourcing of some responsibilities to third parties. However, as discussed in the session, it is crucial to emphasise that outsourcing does not exempt the obliged entity from liability. Thus, collaborators must be rigorously selected, ensuring careful verification and assessment of their expertise and competence.

2. Future challenges: The new European regulatory package

This year, the EU's Official Journal published a new set of AML/CTF measures introducing fresh challenges for the Fintech sector.

The legislative package includes two regulations directly affecting obliged entities:

1. **Regulation (EU) 2024/1624** of the European Parliament and of the Council of 31 May 2024, concerning the prevention of the use of the financial system for money laundering or terrorist financing (hereinafter "Regulation (EU) 2024/1624").

2. **Regulation (EU) 2023/1113** of the European Parliament and of the Council of 31 May 2023, regarding information accompanying transfers of funds and

certain crypto-assets, amending Directive (EU) 2015/849 (hereinafter “Regulation (EU) 2023/1113”).

Additionally, there are two regulations applicable to Member States, indirectly affecting obliged entities:

1. **Regulation (EU) 2024/1620**, establishing the EU Anti-Money Laundering Authority (AMLA), applicable from 2025, with direct supervision beginning in 2028.
2. **Directive (EU) 2024/1640**, requiring Member States to establish mechanisms for preventing the use of the financial system for money laundering or terrorist financing, with transposition deadlines by July 2027.

3. Key changes in the Fintech sector:

Fund transfers regulation amendments (Regulation (EU) 2023/1113):

Effective from 30 December 2024, it introduces the “Travel Rule,” requiring all crypto-asset service providers involved in transfers to collect and make accessible information about the originators and beneficiaries of virtual asset or crypto-asset transfers.

Regulation (EU) 2024/1624:

Applicable from July 2027, it expands the list of obliged entities to include crowdfunding platforms, crypto-asset service providers, mortgage credit intermediaries, and non-financial consumer credit providers.

Introduces new roles such as the “AML Compliance Officer,” a board member responsible for ensuring AML/CTF compliance, and the “AML Compliance Manager,” tasked with implementing daily controls and serving as the primary contact for authorities.

Creation of the EU AML Authority (AMLA):

Operational from 2025, it will directly supervise high-risk cross-border financial entities present in at least six Member States and ensure consistent EU-wide application of AML/CTF rules.

National anti-money laundering mechanisms (Directive (EU) 2024/1640):

Grants centralised Real Ownership Registers the power to conduct inspections and impose sanctions. Establishes interconnected mechanisms for identifying individuals or entities controlling bank accounts or safe deposit boxes, operational by July 2029.

Conclusions and final reminders

While the Fintech sector has driven innovation in finance, creating new business opportunities and improving user experience, it has also increased vulnerabilities in AML/CTF systems. Fintechs must prepare to address current and future AML/CTF challenges by adopting one of two approaches: minimal formal compliance, risking significant regulatory breaches and reputational harm, or genuine commitment to AML/CTF, which avoids penalties and enhances societal contribution by dismantling organised crime networks reliant on illicit funds.

The continual evolution of technologies and financial crime modalities necessitates regular adaptation of controls and procedures. As reflected in the new European regulations, international cooperation and harmonisation of rules are fundamental in combating these crimes.

In summary, the Fintech sector's AML/CTF actions can positively impact society by contributing to a safer, more transparent, and ethical environment, fostering user trust, encouraging greater use of their services, and promoting a sustainable and crime-free business ecosystem.