PREPARING FOR 2025

Navigating Key Changes in EU Financial Crime Regulations

A resource by:

Fourthline × FINTRAIL

Key EU Regulatory Changes in 2025

2025 is a key year for regulatory developments in the EU across financial crime, digital identity, and operational resilience. Staying on top of and implementing the new requirements will require careful planning and coordination, so it's a good idea for financial institutions (FIs) to start thinking now about what the new regulations mean for them. This is also good advice for firms based outside the EU – regulators in other jurisdictions will be monitoring the outcomes, which may influence new regulations in other markets.

1. The EU's Anti-Financial Crime Package

2025 sees the introduction of the EU's long-awaited AML reform package, first proposed in 2021. There are several parts to this package including a new regulation and directive, and the establishment of the Authority for Anti-Money Laundering and Countering the Financing of Terrorism (AMLA), which will launch on July 1, 2025.

AMLA is a decentralised EU agency that will coordinate national authorities to ensure AML/CTF rules are applied consistently. The aim is to address regulatory gaps between member states that have previously been exploited to enable illegal financial flows. AMLA will directly supervise around 40 high-risk FIs, mostly larger firms operating cross-border. It will also coordinate with national financial intelligence units, and standardise regulations and practices by creating a single EU AML/CTF rulebook.

Another pillar of the reform package is Regulation (EU) 2024/1624 (AMLR) and Directive (EU) 2024/1640 which introduce the sixth edition of the EU's Anti-Money Laundering Directive. 6AMLD will introduce new measures around enhanced due diligence, cash payment limits and beneficial ownership among others, and will expand the list of obliged entities to include most of the crypto sector, traders of luxury goods, and professional football clubs. The directive must be transposed into national legislation by July 2027, except Article 74 on the accessibility of information in central beneficial ownership registries, which must be transposed by July 2025.

Unlike previous EU AML directives, the AMLR and the forthcoming technical standards which AMLA will draft in 2025 will apply directly throughout the EU, meaning local requirements derived from national laws may need to be repealed. While the new requirements do not come into effect immediately, firms can get ahead by anticipating changes to policies and procedures and rolling out communication to staff across 2025.

Key Takeaways

- **FIs must make sure they can meet upcoming AML/CTF provisions around:**
  - Stricter customer due diligence requirements for occasional transactions
  - New definitions of 'customers' for CDD purposes in relation to payment initiation service providers
  - Additional enhanced due diligence measures when handling high-value assets for high-net worth individuals
  - Enhanced due diligence measures for occasional transactions and business relationships involving high-risk third countries
  - Detailed requirements to identify and report beneficial owners, based on the components of ownership interest and control
  - New EU-wide limit of €10,000 for cash payments

- **Automated decisions:**
  The AMLR states that firms may adopt decisions resulting from automated processes but that decisions to enter into or maintain a business relationship with a customer must be subject to "meaningful human intervention" to ensure the decision is accurate and appropriate. FIs should consider if their processes are compliant; some firms that have adopted highly automated onboarding flows may need to adapt them to ensure adequate human oversight.

- **Supervision:**
  AMLA will only directly supervise a small number of high-risk FIs, and so the vast majority of firms will not be explicitly affected. However, AMLA will also oversee supervision by national bodies, so in the long term firms may notice some changes to their oversight by national regulators.

2. Payment Services Directive 3 (PSD3)

PSD3 is the latest iteration of the EU's regulatory framework for payment services and e-money. It builds on its predecessor, PSD2, which introduced significant changes such as open banking and strong customer authentication. PSD3 focuses on fraud prevention, digital innovation, and strengthening the role of third-party providers. PSD3 will outline very specific requirements for EU payment firms on fraud and financial crime covering enhanced authentication, transaction monitoring, data-sharing practices, customer risk assessment, and cooperation with third parties.

The regulation is currently being reviewed by the European Parliament and Council, with the finalised version expected by the end of 2024 or early 2025. Once the final text is published, firms will have 18 months to implement the provisions.

Key Takeaways

Firms can get ahead of the upcoming changes by conducting a gap analysis to see where their current authentication processes, ongoing monitoring, data sharing, and security controls may need to be altered to align with the updated requirements:

- Stronger authentication protocols - applying multi-factor authentication (MFA) for all payment transactions, including those initiated through third-party providers. This could involve adopting biometric authentication, dynamic linking, and time-sensitive transaction codes.
- Extending mandatory IBAN verification (known as 'confirmation of payee' in the UK) for all SEPA credit transfers instead of SEPA instant credit transfers only.
- More streamlined authentication for open banking, removing obstacles like requiring users to enter their own IBANs to initiate a payment or access an account, or restricting payments to trusted or domestic beneficiaries.
- New provisions for exchanging fraud data between banks and payment service providers (PSPs), with PSPs allowed to voluntarily share data such as user location, device IDs, spending patterns and payment times to identify trends and suspicious behaviour.
- Enhance transaction monitoring capabilities, including real-time analysis of payment data and automated alerts for suspicious activities.

3. Electronic Identification, Authentication and Trust Services (eIDAS 2)

eIDAS is an EU regulation adopted in 2014 which provides a standardised framework for electronic identification (eID) and trust services. One of its main objectives is to enable cross-border recognition of eIDs, by requiring EU member states to recognise each other's national eIDs, allowing citizens and businesses to access services across borders.

eIDAS2 introduces significant enhancements on the original regulation particularly by establishing a EU Digital Identity (EUDI) Wallet which will provide every EU citizen, resident, and business with a secure and interoperable digital identity wallet, allowing them to store and share various digital identity attributes, including their eID, driving licenses, bank information etc. It also allows them to selectively share information with third parties, giving them full control over their data. eIDAS2 also aims to encourage greater adoption of eID and trust services, for instance by letting people open bank accounts or apply for loans using only a digital identity.

The European Digital Identity Framework which underpins eIDAS2 was adopted in 2024. Member States will be required to offer at least one EUDI Wallet to all citizens and residents by 2026, with the first wallets expected to be made available in 2025. It is expected that financial institutions will need to accept this form of identity verification by 2027.

The potential upsides of the scheme for FIs are considerable. It will introduce a standardised identity verification process that meets KYC requirements across all EU member states, and integrating the EUDI Wallet into onboarding processes could streamline verification efficiency while reducing fraud.

Key Takeaways

If eIDAS2 does promote the uptake of digital identity wallets, FIs may need to decide if the EUDI Wallet can be an addition to their existing onboarding processes or replace part of them. Then they'll need to assess whether the EUDI Wallet can be integrated in a way that is compliant with other regulatory obligations such as the AMLR.

It is unlikely that bank-grade AML compliance can be achieved with a digital wallet alone since, for example, no evidence trail – such as a selfie or device information – is included with eID for a regulator to check. Any changes to a KYC process in this respect must be properly implemented across all policies and procedures with appropriate quality control and systems testing.

4. Digital Operational Resilience Act (DORA)

DORA is an EU regulation aimed at strengthening FIs' digital resilience. Adopted by the European Parliament in 2022 and due to come into force in January 2024, DORA seeks to ensure that the financial sector can operate smoothly even in the event of severe operational disruptions, including those related to cybersecurity and technology failures. The regulation introduces a comprehensive framework that requires FIs and third-party service providers to manage and mitigate ICT-related risks.

Under DORA, FIs must implement risk management frameworks that address potential ICT risks, including cyber risks. This involves setting up procedures for identifying, managing, and reducing these risks, as well as monitoring the resilience of ICT systems. DORA also introduces testing and incident reporting requirements.

In addition, DORA places stringent requirements in relation to critical third-party ICT service providers. These include any party deemed essential to the stability of the financial sector, by providing services or tooling where disruption would impact the operational resilience of FIs, including their ability to meet mandatory compliance obligations. In terms of financial crime, this could include KYC and identity verification services, transaction monitoring services, screening tools, fraud detection tools, or cloud providers that host or process sensitive data including transaction records or KYC data.

Key Takeaways

FIs must implement strong due diligence and continuous monitoring for all ICT third-party service providers including vendors used for onboarding, ongoing monitoring, case management, or reporting. They must evaluate these providers' resilience, ensure contractual safeguards, and maintain contingency plans in case of service failure. Contracts should include provisions to ensure resilience requirements are met, and third parties must be able to demonstrate that they conduct regular testing. FIs should also make sure they have a process in place for sharing information and reporting to regulatory bodies, and notifying them of any breaches.

5. Markets in Crypto-Assets (MiCA) and Transfer of Funds Regulation (TFR)

MiCA is an EU regulatory framework designed to provide clear rules and legal certainty around the issuance, trading, and custody of cryptoassets within the EU. It represents one of the most comprehensive frameworks globally, and is likely to influence other jurisdictions' regulatory approaches going forward. It aims to support innovation and competition in the digital finance space while ensuring strong consumer protections and mitigating financial stability risks.

MiCA was adopted by the European Parliament in 2023, and is designed to take full effect in phases to allow time for regulatory bodies and market participants – including FIs – to adapt to the new rules. Key components set to go live in 2025 include specific licensing and compliance requirements for crypto-asset service providers (CASPs) and issuers of asset-referenced tokens, which will be obliged to obtain authorisation from national regulators from July 1.

Also in the crypto realm, the revised TFR will bring notable changes for EU crypto firms in 2025 Starting in January, all CASPs must collect and share information on both the originators and beneficiaries of any crypto transfer, regardless of the transaction amount. This incorporates the Financial Action Task Force (FATF) 'Travel Rule' into EU law.

Key Takeaways

FIs must understand which assets they handle or which services they offer which fall within MiCA's scope, and consider if they need to obtain authorisation. While MiCA does not directly cover financial crime, crypto activities still fall under the scope of AML/CFT and sanctions regulations, which MiCA strengthens. FIs must ensure that customer due diligence, transaction monitoring, and reporting processes meet both AML and MiCA standards to reduce financial crime risks. Moreover, any FIs offering services to clients who are themselves subject to MiCA should consider whether their existing KYC processes adequately assess their clients' adherence to the new rules.

In terms of the TFR, FIs must be ready to implement processes to identify, verify and record sender and receiver information across both fiat and crypto transactions. Notably, the TFR for crypto applies to all transfers, regardless of the amount, meaning even tiny transactions will have identification and verification requirements, potentially significantly impacting compliance processes.

6. The EU AI Act

The EU AI Act (Regulation (EU) 2024/1689) is a landmark initiative aimed at ensuring safe and ethical artificial intelligence (AI) practices while fostering innovation. As the first comprehensive regulatory and legal framework for AI within the EU, it aims to regulate the development and use of AI, and address various risks associated with AI technologies.

Under the EU AI Act, AI applications will be classified as one of four risk levels:

- **Unacceptable risk:** Applications that pose a significant threat to safety or fundamental rights are prohibited.
- **High risk:** Systems in this category must adhere to strict obligations regarding safety, transparency, and quality. Conformity assessments must be performed before deployment.
- **Limited risk:** Applications in this risk category have few obligations that primarily focus on transparency.
- **Minimal risk:** Generally unregulated, systems in this category face no specific requirements.

The act also includes specific provisions for General-Purpose AI (GPAI) models, which are defined as versatile AI systems capable of performing a wide range of tasks. These models must meet transparency requirements, with additional obligations for those posing systemic risks.

The EU AI Act officially came into force in August 2024, and provisions are currently rolling out. Prohibitions will be enforced within six months, requirements for GPAI will come into effect after a year, and high-risk system regulations will be operational within three years.

Compliance with the act will be enforced by a European Artificial Intelligence Board, which will also facilitate cooperation between EU member states. It will also mandate the formation of national authorities that will be responsible for implementing the regulation.

Key Takeaways

As it sets clear guidelines and obligations for developers and users alike, the EU AI Act will position the EU as a leader in global AI governance.

Organisations operating in or with ties to the EU are encouraged to prepare for compliance with this new regulatory framework. If entities are based outside the EU but have AI systems that affect users within the EU, the regulation will apply to them. As Fourthline services are supported by sovereign AI, Fourthline underlines the importance of complying with the EU AI Act.

All entities that will be required to comply with the EU AI Act should ensure that they have representatives within the EU who can manage compliance. Penalties for non-compliance will be substantial – up to €35 million or 7% of annual global turnover for severe breaches.

Conclusion

To prepare for the significant regulatory changes coming down the track in 2025, FIs in the EU need to adopt a proactive approach. First, they should thoroughly review the provisions and requirements of the new regulations and conduct a gap analysis. Financial crime and fraud teams should ensure that senior management and stakeholders in other teams across business teams, IT, and operations understand the implications in terms of changes to be made and resources required. Educating stakeholders on these changes well in advance of deadlines will help with internal alignment and make the process smoother.

Institutions will need to evaluate and update procedures such as customer due diligence and transaction monitoring, integrating eIDAS2-compliant onboarding processes and supporting the EUDI Wallet for secure verification. Additionally, they should assess their current tech stack's readiness to support enhanced authentication, real-time monitoring, and automated reporting. For any gaps, they could consider third-party providers who can help meet new compliance needs.

Financial crime compliance requires constant innovation to stay ahead of regulatory changes and anticipate emerging risks. Partnering with third parties who are intimately familiar with the regulatory environment – offering either advisory support or technology solutions – can help guide you to ensure smooth adaptation and continued compliance.

How we can help

FINTRAIL

FINTRAIL is a global financial crime consultancy. We've worked with over 100 leading global banks, fintechs and other regulated financial institutions to implement industry-leading approaches to designing onboarding flows and mapping regulations to combat financial crime. With significant hands-on experience, we can help you build, strengthen and assure your financial crime programme to meet evolving regulatory requirements, use technology effectively, and stay competitive.

Visit www.fintrail.com to learn more

Fourthline

Fourthline is a market-leading KYC, AML and financial crime solutions provider. With a single API integration, our modular identity platform enables businesses to solve mission-critical challenges. We combine AI-driven techniques and expert analysis to verify identity documents, biometric data, and applicant information in real-time, ensuring unparalleled accuracy and efficiency. Trusted by banks, online brokers, insurers and leading fintechs, we verify millions of identities for businesses like N26, Nationale-Nederlanden, Trade Republic, flatexDEGIRO, Qonto, Scalapay and more.

Visit www.fourthline.com to learn more