Plenitude
Inspiring confidence, delivering excellence

RegIntel: 2025 Recap and 2026 Outlook Report

Executive Summary 3
Introduction 4
United Kingdom 5
AML/CTF/CPF 5
Key Actions 11
Enforcement 12
Key Actions 15
Fraud 15
Key Actions 18
Sanctions 19
Key Actions 22
Digital Assets 23
Key Actions 25
European Union 26
AML/CTF/CPF 27
Key Actions 30
Enforcement 30
Key Actions 33
Fraud 34
Key Actions 35
Sanctions 35
Key Actions 38
Digital Assets 39
Key Actions 40
United States 42
AML/CTF/CPF 43
Key Actions 46
Enforcement 46
Key Actions 47
Sanctions 48
Key Actions 49
Digital Assets 50
Key Actions 51
Singapore 53
AML/CTF/CPF 54
Key Actions 57
Enforcement 58
Key Actions 60
Fraud 60
Key Actions 61
Digital Assets 62
Key Actions 62

Global 64
Financial Action Task Force (FATF) 64
The Wolfsberg Group 68
Key Actions 69
Conclusion 71
2026 Roadmap 72
Plenitude RegSight 76
Appendix: All 2026 Dates 77

Executive Summary

The financial crime landscape entering 2026 is undergoing profound structural change. Regulatory approaches across the UK, EU, France, and the U.S. are converging around a common theme: accountability over policy intent, demonstrated by practical compliance. Supervisors are moving beyond policy review toward deeper testing of how controls operate in practice, demanding evidence, data integrity, and demonstrable outcomes. At the same time, criminals are exploiting advances in technology, cross-border networks, and digital financial channels to evolve at speed. The result is a global environment where regulation is pragmatic and dynamic, reflecting ever-changing and emerging financial crime risk. This paper focuses on developments across the jurisdictions covered by Plenitude's RegSight tools regulatory registers: UK, EU (including France), US, Singapore and Global.

Several strategic shifts define this new era. Sanctions regimes, particularly in relation to Russia, are widening in scope and intensifying in enforcement, with a growing focus on circumvention, trade flows, and the involvement of new technologies. Corporate transparency obligations are expanding, reshaping how firms verify identity, beneficial ownership (BO), and corporate structures. Fraud, Anti-Money Laundering (AML), sanctions evasion, cybercrime, and crypto risks are rapidly converging, erasing boundaries that once allowed firms to manage them separately.

Technology is both an enabler and a pressure point. Supervisors are adopting Artificial Intelligence (AI), analytics, and SupTech capabilities that raise expectations for firms' own technological maturity. Digital assets and stablecoins are moving into mainstream regulatory frameworks, with stricter demands for governance, substance, and monitoring. AI introduces new risks, synthetic identities, deepfakes, generative fraud, as well as the need for explainability, model oversight, and accountable human control.

In this context, organisations must rethink how their financial crime frameworks operate. The RegIntel Recap and Outlook Paper for 2025/26 distils the year's developments into a set of forward-looking insights and translates them into an integrated operational roadmap for 2026. The roadmap outlines ten core capabilities that firms will need to build or enhance, ranging from unified risk architecture and effectiveness-by-design controls to explainable AI governance, real-time detection, sanctions intelligence, data modernisation, and continuous adaptation mechanisms. These capabilities reflect a shift toward financial crime management that is intelligence-led, data-driven, interoperable, and resilient.

Amidst regulatory change, the firms best positioned for the years ahead will be those that modernise their operating models, strengthen governance, and build systems capable of responding as quickly as risks emerge. Rather than treating regulatory developments as isolated changes, the paper provides a coherent view of how the landscape is evolving and what it will take to operate effectively within it. Its purpose is to support leaders in shaping financial crime strategies that keep pace with accelerating regulatory expectations, technological disruption, and increasingly sophisticated criminal activity.

1 Introduction

As we enter 2026, the global financial regulatory landscape is not only transforming, it is accelerating in complexity, interconnectedness, and operational expectation. This year's RegIntel paper captures a sector at a crossroads, where technological innovation, geopolitical volatility, and regulatory ambition converge.

AI moved from the margins to the mainstream of compliance, with regulators and firms alike grappling with its dual role as both a tool for enhanced detection and a vector for new risks, such as deepfake-enabled fraud and synthetic identity attacks. The regulatory response is increasingly harmonised, with the UK's principles-based approach, the EU's AI Act, and the US's focus on explainability and governance all reflecting a shared imperative: to harness AI's potential while ensuring robust oversight and accountability.

This year also marks a decisive shift in the treatment of data, identity, and transparency. The US's suspension of the Corporate Transparency Act (CTA) for domestic entities, the UK's rollout of mandatory identity verification, and the EU's push for beneficial ownership registers have been key developments. Alongside this, the expansion and tightening of sanctions regimes, driven by geopolitical events and the need to counter circumvention and evasion, is continuing to make sanctions compliance a dynamic and cross-sectoral.

Enforcement and accountability are now at the forefront, with regulators demanding not just policy intent but demonstrable, practical compliance. The move from policy design to operational reality is evident in new offences, heightened enforcement actions, and the expectation that firms can evidence effectiveness in real time. Third-party risk management and supply chain resilience have become non-negotiable priorities, as reliance on external vendors for AI, cloud, and payments infrastructure grows.

Cross-border collaboration and public-private partnerships are now central to regulatory effectiveness, with international cooperation and intelligence sharing underpinning efforts to combat increasingly sophisticated financial crime. At the same time, financial inclusion and proportionality are reshaping risk-based approaches, ensuring that controls are both effective and equitable.

Finally, the increasing regulation of digital assets and instant payments, through frameworks such as Markets in Crypto-Assets (MiCA), the GENIUS Act, and new stablecoin regimes, illustrates that compliance professionals must adapt to a world where innovation, speed, and regulatory scrutiny are inextricably linked.

This paper draws exclusively on the latest developments and insights from 2025–26, providing an authoritative, forward-looking analysis to equip compliance leaders with the knowledge and strategic foresight required to navigate an emerging landscape defined by convergence, complexity, and opportunity.

2 United Kingdom

In 2025, the UK's financial crime and regulatory landscape underwent another year of significant reform, as government, regulators, and law enforcement pushed forward with measures to reinforce corporate transparency, strengthen sanctions enforcement, and address persistent fraud and Money Laundering (ML) risks. The implementation of the Economic Crime and Corporate Transparency Act 2023 (ECCTA) continued to reshape Companies House, culminating in the rollout of identity verification requirements for directors and people with significant control in November.

At the same time, the new corporate offence of Failure to Prevent Fraud (FtPF) entered into force, supported by updated prosecutorial guidance, shifting the balance of accountability firmly onto large organisations.

Sanctions remained at the forefront of UK foreign and economic policy, with the government announcing its largest package since 2022, expanding designations linked to Russia and issuing new sectoral restrictions. The Office of Financial Sanctions Implementation (OFSI) enhanced its enforcement toolkit, issuing penalties and disclosure reports, publishing multiple sector threat assessments, and consulting on tougher civil penalties. In parallel, AML and Counter Terrorist Financing (CTF) regulation advanced through draft reforms to the Money Laundering Regulations (MLRs), a new National Risk Assessment (NRA), and targeted updates to Joint Money Laundering Steering Group (JMLSG) and Financial Conduct Authority (FCA) guidance on politically exposed persons (PEPs).

Fraud and payments reform also featured heavily. The government revised the Payment Systems Regulator (PSR) framework, consulting on its consolidation into the FCA, while the FCA launched a new five-year growth strategy, advanced its safeguarding reforms, and pursued high-profile enforcement actions against firms for financial crime failings. Broader innovation themes emerged too, with new regulation on crypto-assets under consultation, and the FCA exploring how AI can be responsibly tested in financial services. Together, these measures signalled a year where regulatory ambition translated into practical frameworks, enforcement action, and structural change.

For firms operating in the UK, these developments translate into a more demanding operational environment in which compliance expectations are clear, prescriptive and closely scrutinised. Organisations will need to embed enhanced transparency requirements, up-lift fraud frameworks, and implement more dynamic, data-driven approaches to sanctions, AML/CTF and fraud risk management. The increasing use of supervisory "Dear CEO" letters, expanded information-sharing powers and stringent enforcement activity means that firms must ensure their control environments are not only technically compliant but demonstratable effective, well-governed, and responsive to emerging risks. In practice, this requires stronger senior management accountability, tightly integrated FinCrime programmes, and a sustained shift towards proactive risk identification.

2.1 AML/CTF/CPF

Legislation, Regulation, and Guidance

Money Laundering Regulations 2017
UPDATED: Mandatory ID&V Requirement for Directors/PSCs

In August, Companies House confirmed the formal rollout of mandatory ID&V for all new and existing directors and Persons with Significant Control (PSC), marking a major milestone in the implementation of the ECCTA. In line with the November 18th mandatory implementation, amendments were made to Reg.28 and Reg.30A of the MLRs, clarifying

CDD and discrepancy reporting requirements respectively. In newly added Reg. 28(9A), clear definitions are provided for registrable persons, registrable relevant legal entities, and registrable beneficial owners.

For firms, the introduction of identity verification at Companies House also presents an opportunity to enhance the effectiveness of CDD processes. Firms should assess how more reliable Companies House data can be incorporated into onboarding, periodic reviews, and ongoing monitoring processes, particularly in validating the identities of directors, beneficial owners, and controllers. While identity verification at Companies House must not replace independent verification under existing MLRs requirements, it can serve as a complementary data point that strengthens assurance, reduces the risk of inaccuracies, and helps identify discrepancies.

The improvement of Companies House data coincides with authorities continuing to crack down on false registration, with over 11,500 UK-registered companies struck off in a major enforcement operation coordinated by the National Economic Crime Centre (NECC)

2026 Outlook

NEW: Proposed Amendments to the Money Laundering Regulations 2017

In September, the UK Government advanced a comprehensive review of the MLRs, publishing both proposed and draft amendments aimed at modernising the UK's AML framework. The reform package builds on the Treasury's (HMT) 2024 consultation on improving the effectiveness of the MLRs, reflecting the ongoing efforts to enhance the risk-based approach, improve effectiveness, and closer alignment with international standards such as those of the Financial Action Task Force (FATF).

Refining Risk-Based Due Diligence and Information Sharing

The proposed amendments published in September 2025 reflected a more targeted and proportionate approach to due diligence, designed to focus compliance resources on the highest-risk areas. Among the headline reforms, in relation to High Risk Third Country prescribed requirements, firms would be required to apply Enhanced Due Diligence (EDD) only to transactions or relationships involving persons established in FATF "Call for Action" (blacklist) jurisdictions, removing the current blanket application to "Increased Monitoring" (grey list) countries.

The Government also clarified that EDD obligations should apply only to transactions that are unusually complex or unusually large, relative to the given nature of transactions, replacing the previous requirement that captured all complex or unusually large activity. This refinement is intended to reduce unnecessary administrative burden while ensuring enhanced scrutiny is focused on genuinely anomalous or higher-risk transactions which are relative and proportionate to those previously recorded.

Additional proposals introduced new Customer Due Diligence (CDD) obligations on pooled client accounts (PCAs) and set the groundwork for forthcoming guidance on the use of digital identities for customer identification and verification (ID&V). To strengthen coordination across the system, the list of "relevant authorities" able to share information and collaborate on oversight would be expanded, enhancing inter-agency transparency and operational efficiency.

Alongside other proposed updates to the MLRs, these measures reflect a broader effort to sharpen the UK's risk sensitivity, improve collaboration, and provide much-needed clarity in areas of historical uncertainty. Building on this, the Government has also proposed changes aimed at expanding supervisory powers and extending the sectoral scope of the regime.

Expanding Supervisory Powers and Sectoral Scope

In parallel with the targeted amendments to the MLRs, the Government proposed a broader overhaul of the UK's AML/CTF supervisory framework aimed at improving consistency, accountability, and regulatory effectiveness across the system. Central to this reform,

confirmed in September, is for FCA to assume supervision of professional services firms, including legal, accountancy, and trust and company service providers (TCSPs), replacing the current model of multiple professional body supervisors (PBSs). The reform is intended to address long-standing concerns around fragmented oversight, uneven enforcement, and variable supervisory quality.

The Government's wider supervision reforms also propose structural changes to the MLRs themselves, aimed at strengthening the FCA's supervisory powers and expanding the range of sectors brought within scope.
The draft legislation proposed extending beneficial ownership disclosure obligations under the Trust Registration Service (TRS) to newly in-scope trusts and revising registration categories to ensure greater transparency across trust structures.
In the crypto-asset sector, the reforms would broaden the application of the MLRs to encompass a wider range of service providers, with expanded CDD and record-keeping requirements for firms operating in digital asset services. Supervisory authorities would also gain enhanced powers to share information with other public bodies, facilitating stronger cross-system oversight and intelligence exchange.

The draft amendments additionally introduced specific requirements for firms managing PCAs, obliging them to understand the account's purpose, gather information about the underlying customer's business, and assess associated risks. Finally, the proposals would align CDD requirements for letting agents and art market participants (AMPs) with those already applied to high-value dealers (HVDs), closing long-standing regulatory gaps and ensuring consistent AML coverage across sectors.

Subject to Parliamentary scheduling, the amended regulations are expected to come into force during 2026. Firms should prepare for widened CDD obligations, particularly in relation to PCAs and crypto-asset service providers, and anticipate increased supervisory scrutiny as authorities begin exercising their strengthened information-sharing powers. TCSPs, letting agents, and AMPs will need to update their compliance frameworks promptly to ensure readiness once the final amendments are enacted.

Proceeds of Crime Act: UPDATED: DAML Threshold Increased Under POCA

In July, the threshold for submitting a Defence Against Money Laundering (DAML) under the Proceeds of Crime Act (POCA) was increased from £1,000 to £3,000. The change applies to specified firms, including banks, and determines the value of criminal property below which firms may execute customer transactions or return funds when ending a business relationship without committing a ML offence.

The adjustment was introduced to make more effective use of law enforcement and regulatory resources, reflecting evidence that assets previously denied below the £3,000 level were low in both volume and value. In practice, this change gives firms greater flexibility to execute or exit lower-value transactions without submitting a DAML request, reducing delays for customers and internal escalation volumes.

Joint Money Laundering Steering Group (JMLSG) Guidance: UPDATED: JMLSG Guidance on Customer Due Diligence, Governance and Sectoral Expectations

Significant updates to the JMLSG Guidance strengthened the UK's financial crime framework. Covering both Part I and Part II, the revisions align industry practice with supervisory expectations, focusing on proportionate risk management, governance, and sector-specific controls.

Updates to Part I Guidance – Customer Due Diligence, Governance and Digital Verification

Updates to **Part I** provide clearer direction on CDD, electronic identification, and governance. The updates strengthen expectations around how firms identify customers, verify identity, and oversee their AML frameworks.

Key Updates:

- Legal Entities (5.3.129A–C):
  - Introduced discrepancy reporting obligations to identify and report inconsistencies between customer-provided data and the PSC register. Meaning, firms are now expected to actively compare customer information against the PSC register and report material inconsistencies, rather than relying solely on customer-provided data.
  - Enhanced beneficial ownership verification to improve transparency and data accuracy.
- Electronic Identification and Verification (5.3.89):
  - Updated guidance on eID&V to reflect technological developments in digital onboarding.
  - Reinforced use of secure, risk-sensitive verification systems aligned with regulatory expectations.
  - This is particularly relevant to digital onboarding processes, where firms increasingly rely on automated identity checks and biometric verification
- Complex and High-Risk CDD Scenarios (5.3.138A–B):
  - Added new guidance for handling customers or transactions with elevated ML/Terrorist Financing (TF) risk.
  - Enhanced EDD measures should be applied proportionately, based on the specific risk posed by the customer or transaction.
- Ongoing Monitoring and Record-Keeping (5.6.36–5.6.38):
  - Clarified expectations for maintaining current customer data and transaction records.
  - Emphasised continuous monitoring of customer behaviour and risk triggers.
- Governance and Oversight (2.16–2.24):
  - Strengthened requirements for senior management accountability and oversight.
  - Required documented decision-making, clear control ownership, and effective internal challenge mechanisms.
  - These changes reinforce that accountability for AML controls sits with senior management and cannot be delegated solely to compliance teams.

Updates to Part II Guidance – Wholesale Market and Sector-Specific Expectations

Updates to **Part II**, Sector 18 (approved by HMT) introduced detailed guidance for wholesale market participants, addressing high-risk, high-value trading environments. This guidance recognises the higher inherent risk in wholesale markets, particularly where firms deal with complex instruments, layered transactions, and cross-border exposure.

Key Updates:

- Wholesale Market Scope:
  - Expanded direction for firms dealing with complex instruments, layered transactions, and cross-border exposure.
  - Clarified expectations for identifying indirect high-risk relationships and counterparties.
- Transaction Monitoring (TM):
  - Required proportionate monitoring systems tailored to trading activity complexity.
  - Promoted use of data analytics and RegTech to detect anomalies and patterns of concern.
- Client Onboarding:
  - Specified EDD for high-risk clients and intermediaries.
  - Emphasised understanding client structures, source of funds, and beneficial ownership.
- Good Practice Standards:
  - Introduced illustrative examples of effective and deficient AML controls.
  - Reinforced expectations for consistency between policy, control design, and execution.

Financial Conduct Authority (FCA) Guidance

UPDATED: FCA Guidance on the Treatment of Politically Exposed Persons

In July, the FCA published updated guidance on the treatment of PEPs, following consultation on proposed changes conducted between July and October 2024. The revisions were designed to bring greater clarity to firms' risk assessments, reduce unnecessary friction for low-risk customers, and align UK practice with updates to the MLRs.

The guidance clarified key points of interpretation, including that non-executive board members (NEBMs) of central government boards/civil service departments in the UK should not automatically be treated as PEPs. It also introduced greater flexibility on which members of senior management may approve PEP relationships, allowing firms to adopt a proportionate, risk-based approach (RBA). In line with the previously updated MLRs, the FCA confirmed that domestic PEPs should generally be regarded as lower risk unless high-risk indicators are present. Finally, the regulator emphasised that organisations themselves should not be categorised as PEPs unless a PEP is found to exercise significant control.

The revisions were intended to provide firms with clearer boundaries in identifying and managing PEP relationships, while ensuring that compliance resources remain focused on higher-risk cases.

Firms should therefore be calibrating their approach and controls linked to the management of PEPs to reflect the updated guidance, this may also include taking steps to reviewing their existing population of PEPs to ensure that a correct and true picture of risk can be assessed.

AML/CTF/CPF Government and Regulatory Publications

UK Government:

NEW: UK National Risk Assessment of Money Laundering and Terrorist Financing 2025

In July 2025, HM Treasury published the latest ML/TF NRA, a review mandated under the MLRs and conducted every five years. The report provided an updated picture of the evolving risks facing the UK's financial system and outlined areas where mitigation efforts must be strengthened.

The NRA concluded that the overall risk of ML in the UK remains high, with criminals continuing to exploit cash-intensive businesses, complex ownership structures, and professional enablers to obscure illicit financial flows. A notable development since the last assessment in 2020 was the convergence of ML, sanctions evasion, and kleptocracy, with sanctioned individuals increasingly adopting laundering methods traditionally used to move criminal proceeds.

Sector-specific risks were also reassessed. Casinos, electronic money institutions (EMIs), payment service providers (PSPs), and crypto-asset businesses were all identified as carrying elevated ML risks, while EMIs, PSPs, and wealth management services were highlighted as sectors with increased TF vulnerabilities. Firms should consider whether their own risk assessments adequately reflect these evolving threats, particularly where exposure to higher-risk sectors or services exists.

NEW: Second Progress Report on the Economic Crime and Corporate Transparency Act

In June, the UK Government published the second progress report on the ECCTA, outlining the impact of reforms designed to improve the accuracy and reliability of the Companies House register. The report covered the period from March 2024 to March 2025 and highlighted tangible outcomes from the regime's enhanced powers. During the period, 100,400 entities were affected by actions to identify and remove false, misleading, or inaccurate information from the register. Companies House also issued 419 penalty warning notices and 192 penalty notices, demonstrating an increasing willingness to enforce compliance with statutory obligations.

2026 Outlook: With Companies House now exercising enhanced powers more actively, firms should anticipate further tightening of scrutiny in 2026, particularly around beneficial ownership and overseas entity reporting. The move towards mandatory identity verification later in the year will likely mark the next major milestone, and businesses should ensure they are prepared for stricter enforcement of corporate transparency requirements.

NEW: Progress Report on Economic Crime Plan 2

In September, the UK Government published the first outcomes progress report on Economic Crime Plan 2. The report highlighted several key outcomes. Supervisors increased proactive engagement with firms and improved intelligence sharing, with system-wide increases in supervisory and law enforcement disruptions. In terms of asset recovery, authorities seized £243.3 million in criminal assets in the financial year ending 2024. On transparency, the ECCTA introduced wide-ranging reforms, including identity verification for directors and enhanced data-sharing powers for Companies House. Sanctions enforcement also intensified, with 396 recorded sanctions breaches and £24.4 billion in assets frozen, and the expansion of enforcement activity. Finally, public-private collaboration was emphasised through the work of the Joint Money Laundering Intelligence Taskforce (JMLIT), which supported significant operational activity contributing to asset denials of £230.4 million, restraint activity and law enforcement outcomes. These figures signal a more assertive approach by Companies House and suggest that firms should expect increased scrutiny of corporate filings in 2026.

NEW: Rules on Account Closure and Notice Periods

The UK Government announced new rules requiring banks and PSPs to give customers at least 90 days' notice, alongside a clear explanation, before closing an account. The reforms are intended to protect both individuals and businesses from being "debanked" without warning or adequate justification, a concern that has grown following recent high-profile cases. The new legislation being brought forward subject to Parliamentary approval would apply to all PSPs who decide to terminate payment service contracts without a definite expiry date, including bank account closures. They will apply to contracts agreed from and including 28th April 2026, when the legislation is expected to come into force. Firms that fail to comply with the new requirements will face potential enforcement action from the FCA.

Financial Conduct Authority (FCA):

FCA Consultations:

NEW: FCA Consultation on Reforming the Senior Managers and Certification Regime

In July, the FCA launched a consultation on proposed reforms to the Senior Managers and Certification Regime (SM&CR), the framework designed to strengthen individual accountability and reduce consumer harm. The proposals included raising the threshold for firms to be designated as enhanced SM&CR entities, simplifying the Senior Management Function (SMF) approval process, and reducing overlap within Certification Roles (CRs). The FCA also suggested improvements to the efficiency of the 12-week rule, which allows firms to temporarily cover senior management absences without formal approval, and provided new guidance on the allocation of Prescribed Responsibilities, the application of Conduct Rules, and the scope of key SMF roles.

FCA Publications:

NEW: FCA Dear CEO Letter to Wholesale Brokers

In January 2025, following its review of Market Abuse and Money Laundering Through the Markets (MLTM) practices, the FCA issued a 'Dear CEO' letter to wholesale brokers, setting out its two-year supervisory strategy for the sector.

The FCA emphasised three priority areas: broker conduct, culture, and business oversight. The letter underscores the FCA's expectation that wholesale brokers adopt a forward-looking, risk-based approach to compliance, while embedding conduct and cultural standards throughout their operations. Firms that fail to demonstrate adequate progress may face heightened supervisory intervention or enforcement action.

NEW: FCA Feedback Statement on AI and Live Testing

In September, the FCA published Feedback Statement FS25/5 on the use of AI in financial services, summarising stakeholder views and outlining how the regulator's innovation services could support live testing of AI solutions.

Stakeholders broadly supported live testing of AI use cases, particularly in fraud detection, AML, and credit risk modelling. At the same time, respondents highlighted the risks associated with bias, lack of explainability, and governance challenges in AI oversight. Firms called for greater clarity on how existing regulatory frameworks apply to AI, especially regarding accountability, data protection, and decision-making responsibility.

2026 Outlook: Through its commitment to supporting AI innovation, the FCA is operating a Supercharged Sandbox showcase from 28–29 January 2026, where observers can view live AI-led demos, hear from innovators, and engage with the FCA and industry leaders.

NEW: UK Regulatory Approach to AI in Financial Crime Compliance

The UK's regulatory approach to AI in 2025 is defined by a deliberate choice not to regulate AI through a standalone rulebook, but instead to embed AI oversight within the country's existing, principles-based regulatory architecture. This model, championed by the FCA, Bank of England (BoE), and PRA, is designed to remain agile as AI capabilities evolve, while preserving clear lines of accountability for firms deploying AI across their operations. The FCA has been explicit that it will not introduce AI-specific regulations. Instead, AI systems fall under established frameworks. Across the UK regulatory system, explainability is now a core supervisory expectation. For Financial Crime Compliance (FCC), this means firms must be able to articulate why an AI system flagged a transaction, how a customer risk score was generated, and what inputs drove a sanctions match, fraud alert, or AML escalation. With many financial institutions (FIs) outsourcing AI-powered AML, sanctions, fraud, and Know Your Customer (KYC) tools, UK regulators are increasingly scrutinising third-party management, highlighting that outsourcing AI does not outsource responsibility.

Anti-Bribery and Corruption (ABC) Strategy

NEW: 2025 Anti-Corruption Strategy Sets Out UK Government Priorities to Strengthen Integrity and Combat Economic Crime

The UK Government published its 2025 Anti-Corruption Strategy, outlining a renewed commitment to reducing corruption risks across both public and private sectors. The strategy sets out measures to enhance oversight of high-risk sectors, strengthen safeguards in public procurement, and expand the use of digital tools to detect fraud, conflicts of interest, and illicit financial activity. The 2025 Anti-Corruption Strategy signals a renewed focus on prevention, data-driven detection, and closer collaboration between government, regulators, and industry. The strategy also commits to stronger whistleblowing protections and advancing international cooperation to address cross-border corruption threats.

UK AML / CTF / CPF Key actions

01

Strengthen Risk-Based Controls Across the AML Framework

Recalibrate due diligence, monitoring, and escalation processes to ensure enhanced scrutiny is focused on genuinely high-risk customers, transactions, and sectors, aligning EDD, PEP treatment, and crypto-asset obligations with a proportionate, risk-sensitive approach.

02

Prepare for Expanded Regulatory Powers, Supervisory Expectations, and Data Transparency

Upgrade governance, oversight, and reporting frameworks so firms can meet broadened FCA supervision, stronger information-sharing powers, improved Companies House verification, and heightened scrutiny of BO and trust structures

03

Reinforce Operational Readiness for Regulatory Change and Emerging Compliance Requirements

Embed forward-looking operational planning to ensure firms can rapidly adjust policies, technology, and training to upcoming 2026 rule changes, including updated MLRs, strengthened corporate transparency reforms and new account-closure obligations.

2.2 Enforcement

NEW: PSR to be Decommissioned and Integrated into FCA

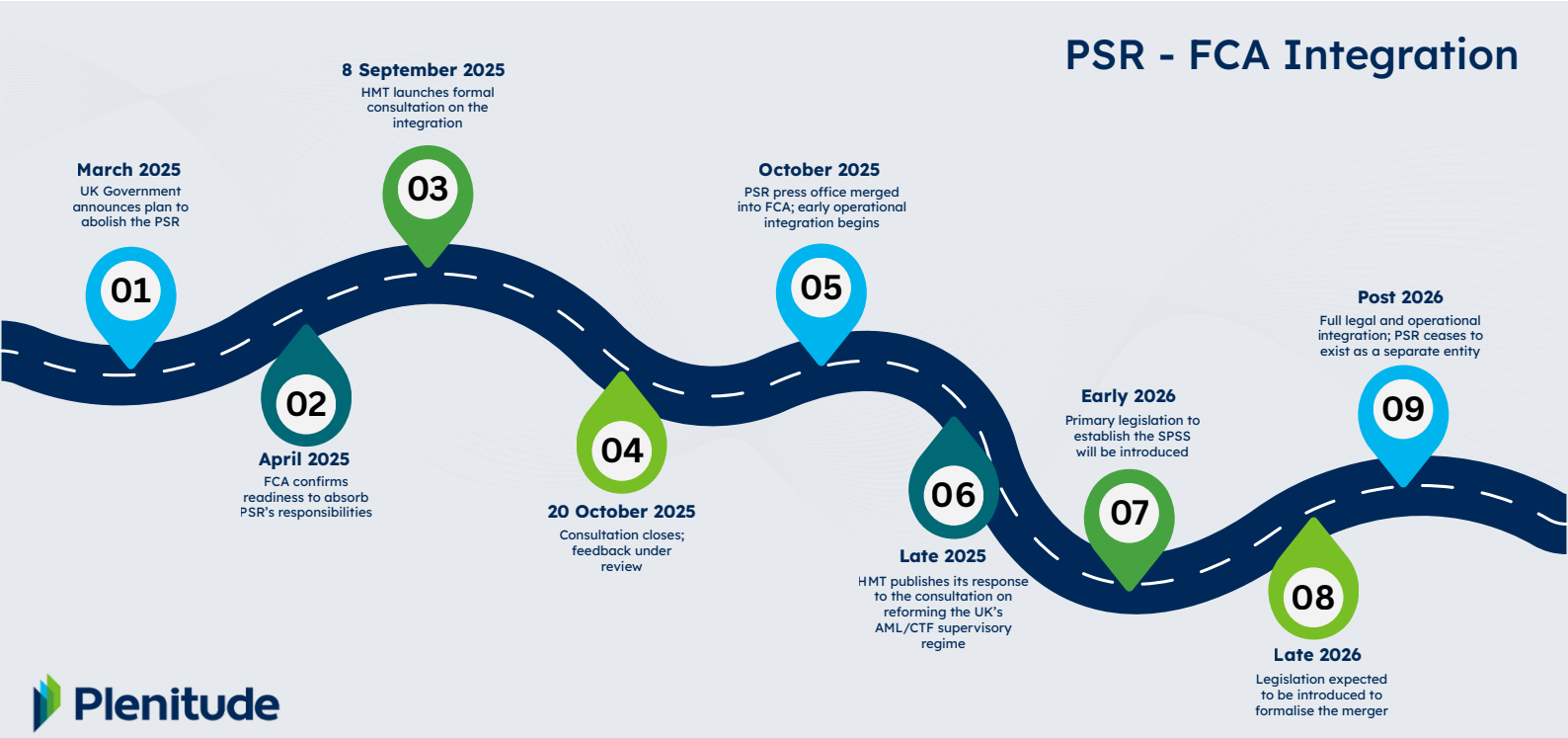
In September, HM Treasury consulted on proposals to integrate the PSR into the FCA, as part of the Government's wider Regulatory Action Plan to simplify the UK's supervisory framework. Following the consultation, the Government confirmed that the PSR will be decommissioned, with its responsibilities transferred to the FCA. Under the proposed reforms, the PSR's responsibilities will be transferred into the FCA, creating a single regulatory touchpoint for firms. The Government stressed that there would be no immediate change to the PSR's supervisory remit or ongoing work, with the integration only taking effect once enabling legislation is passed by Parliament. While firms should not expect immediate changes, they should prepare for a more unified supervisory approach once legislation is enacted.

UPDATED: Government Confirms Single Professional Services Supervisor Model for AML Supervision

In November, HMT published its response to the consultation on reforming the UK's AML/CTF supervisory regime, confirming its decision to pursue a Single Professional Services Supervisor (SPSS) model. A new public body will be established to oversee AML compliance for the legal and accountancy sectors, replacing the current system of multiple PBSs. No changes will be made to the supervision of sectors overseen by HM Revenue & Customs (HMRC), the FCA, or the Gambling Commission, though the Government has committed to improving coordination and consistency across all supervisory bodies. The Office for Professional Body AML Supervision (OPBAS) will be replaced with a new oversight function, responsible for monitoring and supporting the SPSS and statutory supervisors under a strengthened system of governance. The reform aims to address inconsistencies in oversight and enforcement that have arisen under the current fragmented supervision model.

Penalty Actions:

The FCA has continued to intensify its enforcement activity throughout 2025, issuing a series of significant penalties for failings across AML/CTF controls, fraud prevention, and wider governance breaches. Recent enforcement actions highlight recurring themes around weak onboarding controls, ineffective transaction monitoring, and poor governance during periods of rapid growth. While the full list of enforcement actions is available through the FCA's website, notable fines are highlighted below to illustrate the key themes and regulatory expectations emerging from the FCA's 2025 enforcement agenda.



NEW: FCA Fines Monzo £21 Million for Financial Crime Failings

In July, the FCA fined Monzo Bank £21 million for serious failings in its financial crime controls between October 2018 and August 2020. The regulator found that Monzo's frameworks for customer onboarding, risk assessment, and TM were inadequate, particularly as the bank scaled rapidly from approximately 600,000 customers in 2018 to more than 5.8 million by 2022. The FCA highlighted significant lapses, including Monzo's reliance on implausible customer information, such as well-known landmarks listed as residential addresses, and its failure to comply with restrictions imposed in August 2020, which prohibited onboarding high-risk customers. Despite the restriction, the bank signed up more than 34,000 such customers between 2020 and 2022. The case demonstrates the risks of rapid growth without corresponding investment in financial crime controls.

NEW: FCA Fines Barclays £42 Million for Financial Crime Failings

In July, the FCA fined Barclays £42 million for significant shortcomings in its management of financial crime risks, less than a week after announcing a £21 million penalty against Monzo. The case centred on two high-risk client relationships where deficiencies in onboarding and monitoring controls left the bank exposed to facilitating large-scale ML, fraud, and other criminal offences. Barclays were found to have not confirmed that one client was authorised to hold customer funds by checking the Financial Services Register during onboarding, a lapse that ultimately led to customer losses. As part of remediation, the bank agreed to voluntarily pay £6.3 million to affected clients. In another case, weak data collection and monitoring controls allowed a customer to receive over £48 million linked to a major ML operation.

The FCA concluded that Barclays' approach to financial crime risk management fell far short of regulatory expectations, noting that the failings reflected broader cultural weaknesses in how risks were identified, escalated, and acted upon.

Enforcement Operations

NEW: National Crime Agency's (NCA) Operation Destabilise and Machinize Expose the UK's Deepening Fight Against Sophisticated ML

The UK intensified its crackdown on complex, cross-border illicit finance with two major NCA-led operations exposing the scale and sophistication of criminal laundering networks. Operation Destabilise dismantled Russian-linked ML systems facilitating funds for espionage, drug trafficking, ransomware groups, and sanctioned entities, including Russian state-linked organisations. The networks, most notably Smart and TGR, operated across 30+ countries, moving value by swapping crypto (predominantly Tether) for cash, enabling criminals and sanctioned individuals to covertly invest in the UK. The operation led to 84 arrests and the seizure of £20 million in cash and crypto. Complementing these efforts, the NCA's coordinated Operation Machinize targeted hundreds of high street shops suspected of acting as fronts for illegal money transfers, unregistered MSBs, and wider organised crime activity, disrupting another layer of underground financial infrastructure that has enabled criminals to launder proceeds through UK cash-intensive businesses. These operations highlight how criminals increasingly combine crypto, cash-based businesses, and international networks to launder funds. Firms should reassess exposure to crypto-related activity, cash-intensive businesses, and complex cross-border transaction flows.

Regulatory Strategies

NEW: NCA and FCA Publish Joint System Priorities on Economic Crime

In July, the NCA and the FCA published a set of joint System Priorities designed to tackle the most pressing economic crime threats facing the UK. The priorities, aligned to both the UK's NRA and the NCA's National Strategic Assessment (NSA), were intended to help regulated firms allocate resources effectively and strengthen the resilience of the UK's financial system.

Priorities include tackling the role of professional enablers in facilitating ML and sanctions evasion, the misuse of corporate structures and transaction flows by overseas PEPs, and the exploitation of the crypto-asset ecosystem for criminal purposes. Other areas highlighted were the consolidation and cross-border movement of criminal cash, laundering linked to priority jurisdictions, and the large-scale frauds perpetrated by international offenders against UK victims. The use of money mules, the abuse of telecommunications and online platforms to commit fraud, and the financing of terrorism were also identified as systemic risks requiring heightened vigilance.

NEW: FCA 5-Year Growth Strategy

In March, the FCA unveiled a new five-year strategy aimed at deepening trust in financial services, rebalancing risk, and supporting sustainable economic growth. Central to the strategy is a continued emphasis on tackling financial crime, enhancing consumer trust by promoting innovation and improving the quality of support available to retail customers.

Next Steps: Outlined in the FCA 2025/26 Work Programme

- **Enhance Data-Led Supervision**
  - Build advanced, data-driven detection capabilities to identify and respond to financial crime more effectively.
  - Integrate new analytical tools into supervisory processes to improve early risk identification.

- **Strengthen Intelligence Collaboration**
  - Expand partnerships with domestic and international authorities to share data and disrupt organised financial crime.
  - Lead cross-industry work to track and prevent illicit fund flows linked to APP fraud.

- **Elevate Professional Body Standards**
  - Through OPBAS, drive consistent AML standards across the legal and accountancy sectors.
  - Increase scrutiny of supervisory bodies' governance and enforcement practices.

- **Combat Digital Financial Crime**
  - Deploy technology to detect and take down unauthorised financial promotions across websites and social media.
  - Target online fraud networks and strengthen consumer protection in the digital sphere.

- **Embed a Data-Driven Culture**
  - Leverage innovation and RegTech to support efficient, intelligence-led oversight.
  - Reinforce the FCA's strategic shift toward proactive, technology-enabled supervision.

UPDATED: FCA Enforcement Guide and Greater Transparency

The FCA's June Policy Statement PS25/5 introduced a significant shift toward greater transparency in enforcement through updates to its Enforcement Guide, clarifying when the regulator may publicly announce named investigations.

While confidentiality remains the default, the FCA can now make announcements in exceptional circumstances, such as maintaining market confidence, protecting consumers, and preventing widespread malpractice. There are also additional provisions allowing disclosure in cases of suspected unauthorised activity, reactive announcements, or anonymised communications. In limited circumstances, the FCA may now publicly confirm investigations earlier than before, increasing reputational risk for firms, offering insight into decision-making without breaching statutory confidentiality requirements. These reforms aim to enhance accountability and deterrence while balancing fairness to firms and individuals, marking a notable evolution in the UK enforcement landscape.

UK Supervisory and Enforcement Key Actions

01

Prepare for a More Centralised and Coordinated Supervisory Framework

Align governance, oversight, and reporting processes to operate effectively under a more unified supervisory model, anticipating FCA absorption of PSR responsibilities, the creation of the SPSS, and strengthened cross-regulator coordination.

02

Strengthen Financial Crime Controls to Meet Escalating Enforcement Expectations

Reinforce AML, fraud, onboarding, and TM controls to withstand more assertive regulatory scrutiny, responding to themes emerging from major FCA penalties, NCA-led disruption operations, and systemic priorities targeting high-risk customers, intermediaries, and transaction flows.

03

Embed Data-Driven Supervision, Transparency, and Intelligence Integration

Accelerate adoption of data-led supervisory capabilities, enhance intelligence sharing, and prepare for greater public transparency in FCA investigations, ensuring firms can respond to faster, technology-enabled oversight and evolving disclosure expectations.

2.3 Fraud

Legislation, Regulation, and Guidance

Economic Crime and Corporate Transparency Act

NEW: Failure to Prevent Fraud Offence Enters into Force

On 1 September 2025, the new corporate criminal offence of FtPF under section 199 of the ECCTA 2023 came into force, marking a major milestone in the UK's economic crime reform agenda. The legislation forms part of the Government's wider Fraud Strategy, aimed at strengthening corporate accountability and promoting a culture of prevention across large organisations.

The new offence applies to "large organisations", defined as entities meeting at least two of the following criteria:

- More than 250 employees
- Annual turnover exceeding £36 million
- Total assets greater than £18 million

The offence is strict liability, meaning that a company can be held criminally responsible if an associated person, such as an employee, agent, subsidiary, or representative, commits fraud for the organisation's benefit, even if senior management had no knowledge or direct involvement.

To mitigate liability, firms can rely on a statutory defence if they can demonstrate that they had "reasonable procedures" in place to prevent fraud. The Government has issued detailed guidance outlining the principles underpinning this defence, which centre on:

- Conducting a fraud risk assessment tailored to business operations and exposure;
- Implementing proportionate anti-fraud policies, controls, and procedures;
- Ensuring senior management oversight and accountability for fraud prevention;
- Delivering regular staff training and awareness programmes; and
- Establishing clear whistleblowing and reporting mechanisms.

Building on the government's broader drive toward corporate accountability, the Serious

Fraud Office (SFO) and Crown Prosecution Service (CPS) are leading enforcement under the new offence.

Their focus will be on whether firms have maintained and effectively implemented reasonable fraud prevention procedures, rather than isolated incidents of employee misconduct. Updated CPS guidance clarified that corporate liability may arise where a "senior manager" commits or enables fraud within the scope of their authority. Prosecutors will consider governance, self-reporting, and the adequacy of internal controls when determining liability, aligning the new regime with existing "failure to prevent" offences for bribery and tax evasion, and reinforcing a unified approach to corporate integrity.

For firms in scope, the new requirements demand a proactive and holistic response. Compliance teams should review fraud risk assessments, update internal controls, and ensure that policies on conflicts of interest, third-party management, and whistleblowing are fully integrated. Boards and senior executives must take a demonstrable leadership role, evidencing that fraud prevention is embedded within corporate culture, governance, and operational decision-making. By embedding prevention and accountability at the organisational level, the FtPF offence is a transformative step in the UK's fight against economic crime, elevating fraud prevention from a compliance function to a central pillar of corporate governance.

NEW: Public Authorities (Fraud, Error and Recovery) Bill

In December, the UK Government's Public Authorities (Fraud, Error and Recovery) Bill received Royal Assent, it is aimed at strengthening the fight against social security fraud and bolstering the Department for Work and Pensions' (DWP) enforcement toolkit. Under the Bill, FIs must share data with the DWP to help identify potential benefit overpayments, formalising cross-sector information sharing to combat fraud. The DWP will gain expanded investigative powers, including search and seizure, alongside stronger debt-recovery tools allowing direct recovery from individuals who can repay but have previously avoided doing so.

> **"The Bill will strengthen the ability of public authorities to prevent and recover losses from fraud and error, ensuring taxpayers' money is better protected and recovered where misused."**
>
> UK Government Statement via DWP

Government Publications

NEW: Guidance on Countering Public Sector Fraud

In February, the UK Government, through the Public Sector Fraud Authority (PSFA), published new guidance on fraud loss measurement (FLM) as part of the International Public Sector Fraud Forum, working in partnership with the Australian Government and the Commonwealth Fraud Prevention Centre. The framework emphasised the need for strong governance and attributes that organisations must establish to ensure such exercises are carried out consistently and to a high standard. The guidance is positioned not only as a practical tool for common FLM across jurisdictions, but also as a driver for stronger preventative controls and accountability in public sector fraud management.

UPDATED: CPS and SFO Guidance on Corporate Prosecutions

In August, the CPS and the SFO jointly published updated guidance for prosecutors on handling corporate prosecutions, including cases brought under the FtPF offence. The

revisions were designed to clarify how prosecutors should assess corporate liability in the context of evolving economic crime legislation.

Key changes included a refined approach to applying the identification principle, which determines when the actions of senior individuals can be attributed to the company itself. The guidance also set out how prosecutors should approach the FtPF offence introduced under the ECCTA, reflecting the government's drive to expand corporate accountability. In addition, the update revised factors for considering whether prosecution is in the public interest, with explicit reference to the adequacy of a company's compliance programme and the extent of cooperation with law enforcement. The updates highlight that firms can face prosecution where governance frameworks or fraud prevention controls are deemed insufficient.

In parallel, the PSR marked one year since the mandatory reimbursement regime for APP scams went live on 7 October 2024. The data show meaningful progress: around 88% of funds lost in reimbursable APP scams have been returned to victims (equating to about £112m reimbursed) by June 2025, and 84% of claims are now closed within five business days. However, challenges remain, particularly in increasing consumer awareness of the regime, and in ensuring receiving firms pay their share of reimbursements within the required timeframe.

2026 Outlook

NEW: UK Fraud strategy to be published in 2026

The UK Government has confirmed that publication of its long-awaited Fraud Strategy will be pushed back to early 2026, as announced by Fraud Minister Lord Hanson at the UK Finance Economic Crime Congress. The strategy, originally expected by the end of 2025, will set out strengthened protections for consumers and businesses amid escalating scam activity, with a central focus on enhanced cross-sector collaboration between government, financial services, telecoms providers, and technology platforms.

It is expected to place significant emphasis on the deployment of AI and data-driven tools to detect and prevent fraud more effectively. Ongoing debate continues over the extent to which Big Tech firms should contribute financially to fraud prevention efforts, given the volume of APP scams originating from social media and messaging platforms. Rising fraud losses underscore the urgency for reform: banks reimbursed £159 million to victims in the first half of 2025 alone, a 24% year-on-year increase under the new reimbursement rules. Firms should closely monitor forthcoming policy developments and begin preparing for potential shared responsibilities in scam prevention, particularly regarding technological collaboration and enhanced customer protection expectations.

Key Figures

- **4,465** reports of fake FCA scams were received by the FCA's consumer helpline in the first six months of 2025.
- **480** individuals were tricked into sending money to fraudsters.
- In comparison, 2024 saw **10,379** reports and **991** victims who transferred money.

Victim Profile

Nearly **2/3** of reports came from people aged **56** and over, showing older individuals are more frequently targeted.

Common Scam Types

1 Crypto Recovery Scam

Fraudsters claim the FCA has recovered funds from a crypto wallet opened in the victim's name.

2 Loan Scam Follow-up

Victims of loan scams are contacted again by scammers pretending to be the FCA, offering to recover funds for a fee.

3 Purchase Scam

Victims are falsely sold goods or services, which are never delivered or do not even exist.

4 County Court Judgement Scam

Victims are falsely told they owe money due to a court judgement and must pay the FCA.

5 Pig Butchering Scam

Scammers build emotional or romantic relationships, defraud victims through investment schemes, and later impersonate the FCA to offer "recovery" services.

6 'Hey Mum/Hey Dad' Scam

Scammers use social engineering impersonate a victim's child on messaging apps to urgently solicit funds under false pretences.

UK Fraud Key actions

01

Strengthen Ongoing Fraud Prevention Controls to Demonstrate Compliance Under the Now-Operational FtPF Regime

Continuously review and enhance fraud risk assessments, governance, and prevention procedures to evidence that "reasonable procedures" are actively embedded and maintained, ensuring firms can withstand prosecutorial scrutiny under the fully in-force Failure to Prevent Fraud offence.

02

Enhance System-Wide Data Sharing, Collaboration, and Public Sector Alignment to Counter Emerging Fraud Threats

Build the capability to integrate cross-government and cross-industry intelligence, supporting new data-sharing requirements with public authorities, adopting fraud loss measurement methodologies, and preparing for greater joint operational expectations across financial services, telecoms, and technology sectors.

03

Accelerate Adoption of Data-Driven and Technology-Enabled Fraud Detection to Address Escalating Scam and APP Fraud Risks

Deploy advanced analytics, AI, and behavioural monitoring tools to detect complex fraud typologies, improve consumer protection, and meet rising expectations under reimbursement regimes and forthcoming Fraud Strategy reforms.

2.4 Sanctions

Legislation, Regulations, and Guidance

UPDATED: Expansion of Sanctions Reporting Requirements

On 14 May 2025, new reporting obligations under UK financial sanctions legislation entered into effect, extending the scope of firms required to report to OFSI. The expansion brought HVD's, AMPs, letting agents, and insolvency practitioners into scope, significantly broadening the range of industries subject to sanctions compliance requirements.

The reforms were designed to improve OFSI's visibility into how sanctions apply across different sectors, strengthen its enforcement capabilities, and enable more efficient handling of licensing applications. The updated framework also provided greater clarity in areas where firms had previously struggled with legal uncertainty, with amendments made to the Counter-Terrorism (International Sanctions) (EU Exit) Regulations 2019 and the Counter-Terrorism (Sanctions) (EU Exit) Regulations 2019.

By capturing non-financial sectors often exposed to sanctions evasion risks, the UK Government signalled its intention to close compliance gaps and ensure that a wider group of firms are directly accountable for identifying and reporting potential breaches.

UPDATED: OFSI Financial Sanctions General Guidance

In May, OFSI updated its UK Financial Sanctions General Guidance, reflecting changes introduced under the Sanctions (EU Exit) (Miscellaneous Amendments) (No.2) Regulations 2024. The revised framework broadens sanctions reporting obligations beyond financial services, bringing HVDs, letting agents, and insolvency practitioners formally into scope from 14 May 2025. The general guidance sets out updated expectations on reporting designated persons' (DPs) assets, licensing and exemptions, and wider governance requirements, strengthening the overall sanctions enforcement architecture. All changes have been incorporated into Plenitude's RegSight tool, enabling firms to benchmark their readiness.

OFSI also published, sector-specific guidance for HVDs and AMPs to clarify how these new reporting obligations will apply in practice. This guidance confirms that, from May 2025, HVDs must report only where €10,000+ is received in cash, whereas AMPs must report all transactions above the threshold, irrespective of payment method, including those conducted internationally by UK-incorporated firms. The update also clarifies reporting triggers for other newly in-scope sectors, such as letting agents (reporting from the point of instruction) and insolvency practitioners (depending on the nature of their engagement). Although reporting will not apply retrospectively, OFSI expects firms to ensure systems and controls are fully prepared ahead of implementation.

Regime and Sector-Specific Sanctions

NEW: UK Sanctions Regime on People-Smuggling Networks

In a world-first initiative, the UK Government announced a new sanctions regime specifically designed to dismantle people-smuggling networks and disrupt the illicit financing that sustains them. Framed under the Government's "Plan for Change", the sanctions announced in July introduced targeted measures against individuals and entities facilitating irregular migration and organised immigration crime.
The sanctions framework is planned to operational within one year, and focuses on blocking financial flows, freezing assets, and holding smugglers and their enablers accountable. It will be complemented by enhanced operations from the newly strengthened Border Security Command, increased international collaboration, and legislative amendments granting broader powers to UK law enforcement agencies.

NEW: Largest UK Sanctions Package Against Russia Since 2022

In February, the UK Government announced its largest package of sanctions against Russia since the measures introduced immediately after the invasion of Ukraine in 2022. The package designated 107 individuals, entities, and assets, representing a significant escalation in the UK's use of financial and trade restrictions to disrupt Russia's war effort. Those targeted included producers and suppliers of Russian military equipment operating in a range of third countries, as well as senior North Korean officials implicated in the deployment of military forces to Russia. Sanctions extended to wealthy Russian individuals and businesses providing material support to strategic sectors of the Russian economy, and to vessels engaged in transporting Russian oil in breach of international restrictions.

By combining measures against state-linked actors, international enablers, and the logistics underpinning Russia's oil trade, the package underscores the UK's continued commitment to tightening economic pressure on Moscow and reinforcing allied efforts to curtail sanctions evasion. The breadth of the designations reinforces the need for firms to maintain up-to-date sanctions screening, enhanced due diligence on indirect exposure, and vigilance around third-country counterparties and logistics networks.

UPDATED: UK Trade Sanctions on Russian Diamonds and Goods

The UK Government introduced further trade sanctions against Russia, with new measures in effect from April 2025. The update, issued by the Department for Business and Trade, expanded restrictions on the import of Russian-origin synthetic diamonds, including those processed in third countries, bringing the UK into closer alignment with G7 sanctions frameworks. Licencing requirements on goods of concern were tightened, reflecting an effort to close loopholes in supply chains and prevent Russia from sourcing critical components through indirect channels.

The measures signalled a renewed focus on tightening enforcement across global supply chains. Businesses with exposure to high-value goods or complex supply chains should review sourcing, licensing processes, and supplier due diligence to ensure indirect Russian links are identified and mitigated.

Government Publications

NEW AND UPDATED: OFSI Sectoral Threat Assessments

In February, April, June and July, the OFSI published a series of threat assessments across high-risk professional and financial sectors. Each assessment highlighted sector-specific vulnerabilities, underreporting trends, and expectations for stronger compliance following the expansion of UK sanctions obligations.

Financial Services

The OFSI Financial Services Threat Assessment Report highlighted that UK financial firms, especially banks and non-bank payment providers, remain at high risk of sanctions breaches, with over 65% of all suspected breaches since 2022 originating in the sector. It identified rising sanctions-evasion attempts (particularly linked to Russia), widespread weaknesses in frozen-asset handling, due-diligence failures in complex ownership structures, and inconsistent self-reporting by firms.
OFSI concluded that sanctions compliance across financial services remains fragile and requires stronger, more proactive controls, improved reporting, and enhanced monitoring of high-risk customers and transactions.

AMPs and HVDs

OFSI's updated assessment for AMPs and HVDs warned that it remains highly likely that DPs continue to own high-value goods in the UK that have not been reported. The report found likely breaches of asset-freezing prohibitions by Russian DPs and their enablers through dealings in luxury goods, underscoring the art and luxury sectors' appeal for sanctions evasion.

OFSI reinforced that firms must proactively identify and report suspicious holdings, noting that compliance standards across these sectors remain inconsistent despite expanded reporting requirements.

Legal Services

OFSI's legal sector assessment identified persistent vulnerabilities and uneven reporting. Since February 2022, the sector has submitted the second-highest number of suspected breach reports, reflecting both high exposure and risk. Legal service providers, particularly TCSPs, should strengthen due diligence on ownership and source of wealth and ensure timely reporting of suspected sanctions breaches.

OFSI concluded it is "almost certain" Russian DPs are using complex structures to conceal ownership and retain access to frozen assets. Firms were urged to strengthen due diligence, particularly where client ownership or source of wealth is opaque, and to ensure full, timely reporting of suspected breaches.

Property and Related Services

The property sector assessment revealed material weaknesses in sanctions compliance, despite representing only 1% of direct reports to OFSI while accounting for 7% of breaches reported by others. Key concerns included the use of complex ownership structures by Russian nationals to disguise asset control, non-compliance with licence conditions, and underreporting by smaller firms and sole practitioners.

OFSI urged firms to improve due diligence, conduct retrospective reviews, and close reporting gaps, confirming that property-sector compliance remains a supervisory priority.

Crypto-assets

OFSI's crypto-asset sector assessment found it almost certain that UK firms have underreported sanctions breaches since August 2022, largely due to weak detection and escalation processes. Most non-compliance was deemed inadvertent, often arising from indirect exposure to DPs or delayed identification of breaches.
The report also warned that North Korea–linked cyber actors and Iranian networks pose ongoing evasion risks through UK-based crypto-asset providers. OFSI reiterated that sanctions compliance must carry equal priority to AML obligations, with firms expected to invest in robust, technology-led controls.

Key Themes:

Across all sectors, OFSI's 2025 threat assessments point to a consistent pattern of underreporting, limited awareness of sanctions exposure, and gaps in due diligence, particularly where ownership structures or asset control are complex. While sectoral risk profiles differ, several common priorities emerge:

- **Persistent underreporting** of suspected breaches, especially among smaller firms and professional service providers.
- **Use of complex structures** by DPs to conceal control of assets across art, property, and corporate vehicles.
- **Insufficient screening and escalation processes**, often reliant on outdated or manual systems.
- **Growing exposure to state-linked actors** (notably Russian, Iranian, and North Korean networks).
- **Uneven adoption of risk-based compliance frameworks** and weak governance oversight.

NEW: Consultation on Strengthening OFSI's Civil Sanctions Enforcement

In July, HMT launched a consultation proposing significant reforms to the civil enforcement framework administered by OFSI. Key elements included the introduction of indicative penalties for low-level offences in the £5,000–£10,000 range, alongside proposals to reduce voluntary disclosure discounts from 50% to a maximum of 30%, with eligibility tied to early and full cooperation. HMT also proposed an Early Account Scheme (EAS) to accompany a settlement mechanism for unintentional breaches, offering up to a 40% discount for early resolution. Other reforms suggested streamlining reporting and licensing offence processes, while raising the statutory penalty cap from £1 million to £2 million or up to 100% of the value of the sanctions breach.

The consultation marked one of the most substantial proposed shifts in the UK's civil enforcement framework since OFSI's creation, signalling an intention to sharpen deterrence while ensuring proportionality in addressing lower-level breaches. The consultation closed in October, and firms can monitor its development into 2026.

NEW: Cross-Government Review of Sanctions Implementation and Enforcement

In May, the UK Government published a cross-government review of sanctions implementation and enforcement, led by the Foreign, Commonwealth and Development Office (FCDO). The review sought to strengthen compliance across industry, increase deterrence against breaches, and modernise the government's overall sanctions toolkit.

The review recommended consolidating the UK's two separate sanctions lists to support more efficient industry screening and reduce duplication. It also noted that smaller businesses often lack access to specialist sanctions advice, creating awareness and compliance gaps, while existing government guidance was deemed fragmented and in need of modernisation to make it more accessible. The review further identified the need for a cross-government enforcement strategy and the publication of enforcement outcomes to clarify the consequences of non-compliance. Finally, it proposed streamlining reporting points for breaches to reduce confusion and improve transparency.

UPDATED: UK Payments Sector Memorandum of Understanding

The FCA, Prudential Regulation Authority (PRA), and PSR issued the latest revision of their Memorandum of Understanding (MoU), as required annually under the Financial Services (Banking Reform) Act 2013. The updated framework reflects a period of intensified cooperation since 2024, particularly around the implementation of reimbursement rules for APP fraud and joint responses to the challenges posed by digital payments and Big Tech market entrants.

The revised MoU clarified the respective roles and responsibilities of each authority while embedding new principles to guide inter-regulator cooperation. These include greater emphasis on policy alignment, supervisory collaboration, and horizon scanning for emerging risks. In anticipation of the PSR's planned consolidation into the FCA, the MoU also provides continuity by outlining transitional arrangements designed to minimise disruption to firms and the sector.

UK Sanctions Key Actions

01

Strengthen End-to-End Sanctions Reporting, Detection, and Escalation Across All Newly In-Scope Sectors

Embed enhanced reporting processes, screening controls, and breach-escalation mechanisms to meet expanded OFSI requirements, ensuring HVDs, AMPs, letting agents, insolvency practitioners, and other non-financial sectors can accurately identify, verify, and report designated persons, frozen assets, and potential breaches under the broadened regime.

02

Enhance Governance, Due Diligence, and Supply Chain Controls to Address Evolving Geopolitical and Sector-Specific Sanctions Risks

Upgrade governance and due-diligence frameworks to manage heightened exposure arising from new UK sanctions regimes, Russia-related restrictions, diamond and dual-use trade controls, and sectoral vulnerabilities, ensuring firms can identify complex ownership structures, high-risk enablers, and indirect sanctions evasion across financial, art, property, legal, and crypto sectors.

03

Prepare for a More Assertive, Coordinated, and Data-Driven Sanctions Enforcement Environment

Align systems, policies, and cooperation frameworks with the UK's push for consolidated sanctions lists, tougher civil penalties, greater transparency, and cross-government enforcement strategies, building the capability to respond to faster, technology-enabled oversight and strengthened OFSI deterrence measures.

2.5 Digital Assets

Government Publications

NEW: BoE Consultation on Regulatory Regime for Sterling-Denominated Systemic Stablecoins

In November 2025, the BoE published a consultation paper outlining its proposed regulatory regime for sterling-denominated systemic stablecoins. This consultation was published as part of the Government's commitment to establish a comprehensive regulatory framework for crypto-assets and payment innovation.

The BoE proposal sets out a risk-based prudential and payments framework for stablecoins that could pose systemic risks to UK financial stability should their usage scale significantly. Focus areas included authorisation, supervision, and safeguarding rules.

FCA Publications

NEW: FCA and PSR Feedback on Big Tech and Digital Wallets

In February, the FCA and the PSR issued a joint feedback statement on the growth of big tech in payments and the rising use of digital wallets, following the FCA's Call for Information launched in July 2024. The regulators highlighted both the opportunities presented by digital wallets and the increasing financial crime risks that accompany their rapid adoption.

Data from 2023 indicated that around one in five card users were already using digital wallets for the majority of their transactions, a trend expected to accelerate further. While digital wallets offer convenience, their popularity has created additional avenues for scammers to exploit through phishing campaigns and social engineering. The statement reaffirmed that, despite the role of digital wallet providers in facilitating transactions, the underlying card issuers remain responsible for compliance with strong customer authentication (SCA) obligations and, crucially, for reimbursing victims of unauthorised transactions.

The joint statement signals that as digital wallets continue to grow in prominence, the FCA and PSR will increase scrutiny of fraud liability, authentication standards, and the operational resilience of providers, while ensuring card issuers uphold consumer protections in the event of fraud.

NEW: FCA Discussion Paper on Regulating Crypto-asset Activities

In May, the FCA published Discussion Paper DP25/1, setting out potential approaches to regulating a broad range of crypto-asset activities. The paper marked a significant step towards establishing a comprehensive UK regulatory framework for crypto, seeking to strike a balance between encouraging innovation and safeguarding consumer and market integrity.

Among the FCA's proposals were plans to bring activities such as operating crypto-asset trading platforms, intermediation, lending and borrowing, staking, potentially decentralised finance (DeFi) formally within the scope of financial regulation. The FCA invited industry feedback by June, signalling its intention to refine the proposals before moving towards a more formal regulatory framework in 2026.

UPDATED: FCA Confirms Changes to Safeguarding Regime for Payments and E-Money Firms

In August, the FCA finalised new rules and guidance to strengthen the safeguarding regime for payments and e-money firms, a move aimed at improving consumer protection and reducing risks in the event of firm failure. The updated framework clarified areas including how firms are expected to maintain robust record-keeping and ensure oversight of third-party providers engaged in safeguarding arrangements. The FCA also confirmed that firms must notify the regulator of any material safeguarding issues, reinforcing its commitment to closer monitoring and earlier intervention.

NEW: FCA Consultation on Handbook Requirements for Crypto-asset Firms

In September, the FCA published CP25/25, outlining how the FCA Handbook will apply to firms entering the new crypto-asset regulatory perimeter. The consultation proposes extending rules on authorisation, governance, systems and controls, operational resilience, and conduct standards, including senior management accountability under SYSC.
The FCA also explores how Consumer Duty, COBS, PROD, and access to the Financial Ombudsman Service should apply to crypto-asset activities to ensure consistent protections across traditional and digital markets. Structured in two phases with staggered deadlines, the consultation represents a major step toward a fully integrated UK regulatory framework for crypto-asset services. The consultation closed on the 12th of November 2025, outcomes will be expected early 2026.

> **Crypto is a growing industry. Currently largely unregulated, we want to create a crypto regime that gives firms the clarity they need to safely innovate, while delivering appropriate levels of market integrity and consumer protection. Our aim is to drive sustainable, long-term growth of crypto in the UK. We're asking whether we have got the balance right.**
>
> David Geale, Executive Director of Payments and digital finance at the FCA

NEW: FCA Launches Stablecoin Sandbox Cohort

Shortly following the BoE consultation issuance in November, the FCA announced a new Stablecoin Cohort within its Regulatory Sandbox, marking a significant milestone in the UK's efforts to encourage responsible innovation in digital payments.
The cohort enables selected firms to test real-world use cases for GBP-stablecoin payments in a controlled environment, under close FCA oversight. Participants may trial:

- issuance models aligned with forthcoming UK regulatory expectations
- merchant acceptance and payment integration use cases
- custody, wallet, and reserve-asset operational frameworks
- AML/CTF controls aligned with the future risk-based UK crypto regime

The FCA emphasised that testing within the sandbox does not replace eventual compliance obligations. Firms must demonstrate strong risk management, robust consumer protection measures, and alignment with BoE/FCA policy direction as the systemic stablecoin regime evolves.

UK Digital Assets Key Actions

01

Prepare for a Fully Integrated UK Regulatory Perimeter Covering Stablecoins, Crypto-Asset Services, and Digital Wallets

Upgrade governance, authorisation readiness, safeguarding arrangements, and operational resilience to meet emerging BoE and FCA requirements, systemic stablecoin rules, expanded FCA Handbook expectations, and strengthened payment and e-money safeguarding regimes.

02

Strengthen Consumer Protection, Financial Crime Controls, and Liability Frameworks Across Digital Payments and Wallet Ecosystems

Improve fraud prevention, authentication, AML/CTF controls, and liability processes as regulators intensify scrutiny of digital wallets, Big Tech payments, and crypto-asset activities, ensuring firms can manage rising scam risks, uphold SCA obligations, and deliver consistent consumer protections across traditional and digital channels.

03

Build Innovation-Ready, Risk-Managed Capabilities Aligned to the UK's Digital Asset and Stablecoin Sandbox Frameworks

Develop the systems, testing capabilities, and risk management frameworks needed to participate in FCA and BoE sandbox initiatives, ensuring firms can safely innovate with stablecoin issuance, custody, payments, and digital asset infrastructure while demonstrating robust safeguards, transparency, and alignment with future UK regulation.

2.6 Conclusion

UK regulatory change in 2025 built on the momentum established in 2024, with a continued emphasis on implementation and enforcement of previously introduced policy measures. Corporate transparency measures were tightened, sanctions enforcement became more assertive, and fraud prevention moved to the centre of regulatory and prosecutorial agendas. Across AML/CTF/CPF, fraud, and sanctions, the theme was clear: firms must evidence practical compliance, not just policy intent.

As 2026 begins, regulators and government are expected to sharpen supervisory testing of new obligations, from identity verification to pooled client account CDD, while early enforcement of the FtPF offence will set critical precedents. Sanctions will remain a central tool of UK foreign policy, with OFSI equipped to impose tougher penalties and greater transparency. In payments and digital assets, structural changes, including the proposed integration of the PSR into the FCA and the rollout of crypto-asset regulation, will continue to reshape the regulatory landscape.

For firms, the year ahead will demand continued adaptability, investment in governance and technology, and proactive engagement with regulators. Those able to demonstrate robust frameworks, transparent operations, and effective fraud prevention will be best placed to navigate what is set to be another transformative year in the UK's evolving fight against financial crime.

3 European Union

2025 marked a decisive pivot in the European Union's approach to financial crime, where previously announced reforms became increasingly operational. The launch of the Anti-Money Laundering Authority (AMLA) in Frankfurt symbolised the start of a new era: one defined by centralised oversight, greater consistency across Member States, and a more assertive regulatory stance.

Around this institutional shift, regulatory momentum accelerated. The European Banking Authority (EBA) advanced consultations on the Regulatory Technical Standards (RTS) that will underpin AMLA's operational model, including risk assessments, criteria for direct supervision, CDD expectations, sanctions enforcement, and supervisory tools. Elsewhere, debates continued to surround the EU's high-risk third-country list, reflecting tensions between reliance on FATF assessments and calls for a more autonomous EU risk lens. In parallel, successive sanctions packages against Russia, spanning trade, technology, financial services, digital assets, and enforcement mechanisms, signalled the bloc's determination to tighten controls and close circumvention channels.

The digital assets landscape also entered a new phase of regulatory maturity. MiCA's phased implementation moved forward through the "grandfathering" period, while European Securities and Markets Authority (ESMA) issued supervisory briefings and public statements to ensure consistent authorisation of Crypto-Assets Service Providers (CASPs), curb outsourcing risks, and limit access to non-compliant stablecoins. The EBA's opinion on ML/TF risks further underscored vulnerabilities in crypto-asset relationships, governance frameworks, outdated sanctions screening, and the oversight of RegTech and AI tools, areas where rapid business growth has often outpaced institutional control environments.

At the same time, the EU's enforcement posture sharpened. Infringement proceedings were launched against Member States failing to transpose the 6th Anti-Money Laundering Directive (AMLD) on schedule, whilst Europol's threat assessments and cooperation guidelines reinforced the need for closer public-private collaboration.

France mirrored and amplified these trends through its own multi-layered regulatory and supervisory agenda. Legislative reforms extended tax transparency and financial crime obligations to CASPs; updated ACPR–Tracfin guidelines strengthened CDD and reporting expectations; and national sanctions guidance was consolidated to improve clarity and compliance. Tracfin and the Ministry of Justice intensified enforcement against laundering networks, while the Autorité de contrôle prudentiel et de resolution's (ACPR) supervisory work programme addressed AML/CFT risks in crypto-assets and DeFi. Revisions to the list of non-cooperative tax jurisdictions, new measures targeting drug trafficking and ML-linked offences, and prominent enforcement actions across banking and asset management further underscored France's commitment to addressing both domestic vulnerabilities and cross-border threats.

Together, these developments reflect a European landscape undergoing simultaneous consolidation, convergence, and escalation. The EU is moving from fragmented national approaches toward a more harmonised, technology-enabled, and enforcement-driven model, one where supervisors expect stronger governance, more dynamic monitoring, credible oversight of AI and RegTech, and resilient controls across both traditional and digital financial channels. Firms now operate in a regulatory environment that is both more integrated and more demanding, with expectations shaped not only by new rules but by a new intensity in how they are applied across the Union and within France.

What this means in practice

Financial crime compliance controls need to not only be in place, but shown to work. Firms should be ready to evidence effectiveness, not intent. In practice, this means ensuring:

- Information held on customer, product, and transactions is reliable and current.
- Monitoring and screening systems are robust.
- Governance of AI, RegTech, and outsourced functions is strong.
- Risk assessments and control mapping are refreshed to reflect changing risk exposure.

The practical shift is simple: regulators expect controls that are **explainable**, **evidenced, and operationally robust**, and they will increasingly verify this through deeper, data-led supervision.

3.1 AML/CTF/CPF

European Union

UPDATED: EU High-Risk Third-Country List

Mid-2025 saw the European Commission take a significant step in tightening its grip on financial crime risks beyond EU's borders. The Commission revised its list of high-risk third-country jurisdictions with strategic deficiencies in their AML/CFT frameworks, aligning the list more closely with the FATF process. The update, which came into force on 5 August 2025 via amendments to Commission Delegated Regulation (EU) 2016/1675, added Algeria, Angola, Côte d'Ivoire, Kenya, Laos, Lebanon, Monaco, Namibia, Nepal, and Venezuela to the list. Barbados, Gibraltar, Jamaica, Panama, the Philippines, Senegal, Uganda, and the United Arab Emirates (UAE) were removed following evidence of regulatory improvements.

For EU-regulated entities, this means EDD is now required for relationships and transactions involving the newly listed jurisdictions and updates to geographic risk assessment methodologies. The changes reflected the FATF's "jurisdictions under increased monitoring" list at the time.

However, the move was not without controversy. The European Parliament (EP) objected to the Commission's reliance on the FATF methodology, arguing that the EU's approach should reflect the specific risks of its internal market rather than depend heavily on external assessments. The removal of the UAE from the list proved particularly contentious, despite its removal from the FATF Grey List in February 2024, with the EP questioning whether sufficient reforms had taken place given the EU's deepening economic ties with the country. Concerns were also raised about Russia's continued omission from the list, despite widespread evidence of proliferation financing (PF), cyber threats, and extensive EU sanctions. In response, the Commission adopted a new Delegated Regulation, inserting a review clause that obliges the Commission, by 31 December 2025, to assess third countries not currently subject to FATF monitoring but whose FATF membership has been suspended, to determine whether amendments to the EU high-risk list are warranted. The review ultimately led the EC to add Russia to the list of high-risk countries in December, citing strategic deficiencies in its AML/CTF framework.

NEW: European Commission (EC) Launches Infringement Proceedings over 6th AMLD

In September, the EC made it clear that delays in implementing AML rules would not go unnoticed. It launched infringement proceedings against 11 EU Member States for failing to transpose key provisions of the 6th AMLD (Directive (EU) 2024/1640) by the deadline of 10 July 2025.

The Directive is a central part of the EU's wider AML/CFT reform package and introduces major new requirements, most notably, ensuring comprehensive access to beneficial ownership information (BOI). Member States are now obliged to guarantee that data on legal entities, trusts, and similar arrangements is made available to competent authorities, Financial Intelligence Units (FIUs), and those able to demonstrate a legitimate interest.

The Commission's action reflects the wider EU objective of promoting a common regulatory approach. Member States were given two months to address the deficiencies or face the issuance of a formal reasoned opinion, the next step in EU infringement procedures.

> **70% of competent authorities report high or rising ML/TF risks in the financial sector. They point to weak AML/CFT controls and poor governance, as firms appear to prioritise growth over compliance.**
>
> EBA Press Release

NEW: EBA Opinion on ML/TF Risks in the EU Financial Sector

In May, the EBA took a closer look at the evolving risks of ML/TF risks across the EU's financial sector. Drawing on data collected between January 2022 and December 2024 from national competent authorities (NCAs), supervisory databases, and regulatory activities.

Key risks identified include:

- **Controls in PSPs and FinTechs not keeping pace with rapid growth**: Many PSPs and FinTechs are expanding faster than their financial crime controls can mature, resulting in gaps across onboarding, monitoring, and governance. Firms operating in fast-growing segments must demonstrate that compliance functions scale proportionally as regulators will expect evidence of forward-looking resourcing and control planning.

- **Weak monitoring of relationships with CASPs**: The EBA highlighted deficiencies in how firms oversee interactions with CASPs and crypto-linked FinTechs, including insufficient ongoing monitoring and unclear understanding of counterparties' risk profiles. Firms should expect supervisory scrutiny around crypto exposures and must strengthen due diligence and lifecycle monitoring of any crypto-adjacent relationships.

- **Lack of in-house expertise to oversee RegTech and AI tools**: Many firms were unable to effectively challenge, validate, or oversee the RegTech and AI systems used in AML/CTF processes. This includes gaps in understanding model behaviour, limitations, and data dependencies. Firms must build internal technical competence and reinforce model governance, or risk operating critical tools that cannot be adequately supervised or defended to regulators.

- **Outdated sanctions screening systems**: The EBA found that many firms still rely on "static" sanctions engines that are slow to update and poorly calibrated for today's fluid geopolitical environment. Implication: Firms need to move toward more dynamic, automation-enabled screening architectures that can adjust quickly to list changes and reduce false positives while maintaining accuracy.

- **Inadequate escalation procedures for potential breaches**: Weak or inconsistent escalation pathways mean that sanctions or monitoring alerts are not reliably reviewed, investigated, or resolved in a timely way. Firms must tighten governance of escalation routes, strengthen case management workflows, and ensure clear ownership for decision-making to prevent regulatory breaches.

- **Governance weaknesses across AML and sanctions frameworks**: Taken together, the EBA's findings signal systemic issues in governance, fragmented oversight, insufficient board engagement, and limited cross-functional coordination. Firms should prepare for heightened supervisory testing of governance structures, including board awareness, documented oversight, and evidence of effective challenge.

France

> **In 2024, Tracfin received 215,410 reports, including 211,165 suspicious transaction reports (STRs), marking a 13% increase from 2023.**
>
> Tracfin, Rapport d'activité 2024, Ministère de l'Économie

Legislation, Regulations, and Guidance

NEW: Legislative Reforms Targeting Drug Trafficking and Related Offences

In June, France strengthened its tackling of drug trafficking and organised crime through the adoption of Law No. 2025-532. The reforms expanded the legal framework for prosecuting drug trafficking, while also reinforcing provisions related to ML and corruption.

Notably, the law grants French authorities enhanced powers to disrupt illicit financial flows, including the ability to freeze funds and economic resources belonging to individuals directly involved in drug trafficking or acting on behalf of those implicated.

The legislation underscored France's determination to tackle drug-related organised crime not only through criminal sanctions but also by targeting the financial infrastructure underpinning trafficking networks.

UPDATED: ACPR and Tracfin Joint Guidelines on Due Diligence and Reporting

In April, the ACPR and Tracfin issued an updated version of their joint guidelines on CDD and reporting obligations. The revisions were designed to reflect the current regulatory framework and place greater emphasis on the detection and assessment of unusual transactions, as well as the escalation or dismissal of suspicions to ensure the quality of STRs.

The guidance clarified processes of detecting and assessing unusual transactions, and on how suspicions should be escalated or dismissed to improve the quality of STRs. The guidelines also explored emerging risks in ML/TF, urging firms to adapt their detection tools to keep pace with evolving criminal tactics. Through these updates, the ACPR and Tracfin reinforced their expectation that firms adopt a more dynamic and risk-sensitive approach to due diligence and reporting, ensuring both regulatory compliance and the effective disruption of illicit financial activity. The update reflects a broader global shift toward enhancing the quality of robustly and effectively identifying, analysing, and reporting suspicious activity.

EU AML Key Actions

01

Prepare for AMLA Direct and Indirect Supervision

Align internal frameworks early so the firm can evidence readiness. This includes reviewing governance structures, reviewing the draft RTS to identify any operational impacts.

02

Integrate AMLA– European Supervisory Authorities (ESA) Cooperation into Compliance Planning

Ensure internal frameworks mirror the ESAs' push for convergence so the firm presents consistently across sectors and jurisdictions.

02

Enhance Use of Technology in Compliance Frameworks

Ensure the use of new technologies are governed, explainable, and defensible. Tools should be calibrated according to regulatory requirements and measured risk.

03

Strengthen FIU Engagement and Information Sharing

Improve the speed, accuracy, and evidentiary quality of suspicious activity intelligence shared with FIUs.

3.2 Enforcement

The EU enters 2026 with a more coordinated and intelligence-driven AML/CFT framework, shaped by structural reforms rather than headline enforcement. Europol's 2025 EU-SOCTA heightened supervisory focus on corruption risks, cyber-enabled financial crime, and the rapid adoption of AI by criminal groups, while the EBA's SupTech work signalled a clear move toward data-led, technology-enabled supervision. Most significantly, the launch of AMLA established a centralised authority to harmonise expectations and strengthen oversight across Member States. Together, these developments point to a supervisory environment that will prioritise operational effectiveness and real-world outcomes over procedural compliance.

European Union

NEW: Europol Practical Guide on Cooperation with Financial Institutions

In February, Europol published a Practical Guide for Operational Cooperation between Investigative Authorities and FIs, aimed at strengthening the fight against financial crime through enhanced cross-sector collaboration.

The guide underscores the benefits of structured cooperation, including:

- Improved investigative outcomes
- Higher quality Suspicious Activity Reports (SARs)
- Enhanced understanding of cross-border financial flows

It also sets out practical methods and scenarios of cooperation, highlighting opportunities for engagement ranging from real-time intelligence sharing to coordinated analysis of emerging risks. By providing both operational frameworks and illustrative case studies, the guide is designed to help FIs and investigative authorities institutionalise best practices and encourage more effective partnerships across jurisdictions, with learnings that can be gained from both firm and authority levels.

NEW: Europol EU Serious and Organised Crime Threat Assessment 2025

In March, Europol released the latest edition of its EU Serious and Organised Crime Threat Assessment (EUSOCTA), drawing on intelligence from EU member states and international law enforcement partners to anticipate future organised crime risks.

Key threats include:

- **Organised crime increasingly undermines societal and financial system foundations**: Criminal networks are exerting deeper influence through illicit financing, ML, corruption, and support to hybrid threat actors.
- **Digital infrastructure exploited for cyber fraud, ML, and ransomware**: Criminals are leveraging digital platforms and online payment channels to scale fraud and ML schemes.
- **Rapid adoption of AI by criminal groups**: AI is used to automate social engineering, generate synthetic identities, impersonate FI's, and orchestrate large-scale fraud and laundering operations.

> **"The insights provided by the EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025 will shape strategic decision-making, operational priorities, and legislative developments to strengthen the EU resilience against serious and organised crime"**
>
> Catherine De Bolle Executive Director of Europol

NEW: EBA Report on SupTech in AML/CFT Supervision

In August, the EBA published a report on the use of advanced technology tools in AML/CFT supervision, drawing on a survey of NCAs and discussions held during a dedicated SupTech workshop. Reported benefits of adoption include improved data quality, enhanced analytics, stronger decision-making, greater operational efficiency, and more robust risk assessments, alongside opportunities for increased collaboration between supervisors.

The report also highlighted several challenges to adoption, ranging from persistent data quality issues and governance limitations to legal uncertainties, accountability gaps, resource constraints, and institutional resistance to change. To address these barriers, the EBA outlines a series of good practices designed to help NCAs and firms harness SupTech effectively, overcome implementation challenges, and maximise its supervisory benefits. Firms should ensure their technological infrastructure can generate high-quality, explainable, and timely data to meet these evolving supervisory expectations.

NEW: Establishment and Early Work of the EU AMLA

Priorities, Leadership, and Early Work

The AMLA formally began operations in Frankfurt on 1st July 2025, marking significant institutional reform to the Union's AML/CFT supervisory structure. AMLA's mandate centres on three core responsibilities:

- Direct supervision of selected FIs identified as presenting the highest ML/TF risks, combined with indirect oversight of other entities through national competent authorities (NCAs);
- Coordination and support of FIUs across the EU; and
- Development of technical standards, regulatory guidance, and supervisory practices to strengthen consistency across Member States.

In June, AMLA also signed a MoU with the ESAs - the EBA, ESMA, and the European Insurance and Occupational Pension Authority (EIOPA). The agreement established a framework for cooperation and structured information exchange, aiming to promote supervisory convergence, enhance intelligence sharing, and build supervisory capacity across sectors. This integration underscores AMLA's role at the centre of the EU's financial crime architecture.

Later in the year, AMLA published its first Work Programme, "From Vision to Action," outlining priorities for the remainder of 2025. These include beginning strategic planning for future operations, launching indirect supervisory work with NCAs and direct supervisors, finalising and operationalising the EU FIU framework, and collaborating with EU FIs on the development of new AML/CFT standards. AMLA also committed to building the internal resources and institutional capacity needed to sustain its ambitious mandate.

The launch of AMLA signals a new phase of EU AML/CFT supervision, characterised by greater centralisation, enhanced consistency, and stronger enforcement capacity across Member States. As the authority builds momentum, firms can expect more uniform supervisory expectations, increased scrutiny of high-risk entities, and closer coordination between national and supranational supervisors.

AMLA Mandates

In March, the EBA launched a consultation on proposed RTS presenting standards for assessing inherent and residual risk, the criteria for determining entities under AMLA's direct supervision, and expectations around CDD. They also proposed rules on pecuniary sanctions, administrative measures, and enforcement payments, illustrative of the forthcoming alignment of supervisory methodologies and enforcement tools under one framework.

In October, the EBA issued technical recommendations on structuring AMLA's supervisory and coordination functions. Key recommendations covered methodologies for supervision, responsibilities of joint supervisory teams, criteria for assessing EU law breaches, and approaches to engagement with other international supervisors. In September, the EC announced that Level 2 acts, which include RTS and implementing technical standards, will be deprioritised until at least 1 October 2027. In a letter to the three ESAs and AMLA, the Commission explained that non-essential acts would not be adopted before that date due to the regulatory complexity and cost.

Following the consultations and recommendations, AMLA adopted two sets of RTS, one establishing criteria for selecting institutions for direct supervision and another defining the methodology for assessing ML/TF risk, and simultaneously launched a consultation on ITS to strengthen cooperation within the AML/CFT supervisory system.

Amidst these ongoing changes, firms should continue to prepare for AMLA's more centralised oversight model while maintaining flexibility to adapt once the final rulebook and RTS framework are adopted.

> **Money laundering corrodes public trust, fuels organized crime, corruption, and tax evasion, and distorts fair competition… Our response must be strong and unified.**
>
> Bruna Szego (AMLA Chair), European Anti-Financial Crime Summit, Dublin, 7 May 2025

France

NEW: ACPR Programme of Work 2025

In January 2025, the ACPR set out its supervisory roadmap for the year, informed by a broad risk assessment of the French financial system. The ACPR outlined several strategic priorities including strengthening AML/CFT oversight,placing particular emphasis on the risks posed by crypto-assets and DeFi, and advancing a more proportionate, risk-based supervisory approach.

The ACPR's heightened focus on digital asset-related risks reflects the growing systemic importance of crypto markets and aligns with the implementation of EU-wide frameworks, including MiCA and the Transfer of Funds Regulation (TFR). Firms operating in these segments should expect increased supervisory scrutiny of their governance, risk management, and AML/CFT controls in 2026.

NEW: Union Bank of Switzerland (UBS) Settles Legacy Tax-Evasion Case in France

In September, UBS agreed to pay €835 million in fines and damages to settle a long-running French tax-evasion case, marking the conclusion of one of Europe's most significant financial crime proceedings. The case centred on UBS's cross-border activities between 2004 and 2012, during which the bank was found guilty of unlawful client solicitation and aggravated ML, allegedly helping wealthy clients conceal assets and evade French taxes. The outcome underscored France's sustained commitment to pursuing legacy cases involving tax evasion and ML.

EU Enforcement Key actions

01

Anticipate Supervisory Action on Fraud and AML Weaknesses

Prepare for more intrusive, risk-led interventions by ensuring control environments can withstand real-time supervisory testing.

02

Support Cross-Border Enforcement Coordination

Build the internal infrastructure necessary to cooperate effectively with multi-jurisdictional investigations and sanctions enforcement.

03

Enhance Public–Private Collaboration

Strengthen relationships with law enforcement and supervisory bodies to better detect and disrupt complex financial crime.

3.3 Fraud

European Union

NEW: Instant Payments Regulation

The Instant Payments Regulation (Regulation (EU) 2024/886), implemented in phases throughout 2025, represents a major milestone in the modernisation of the EU's payments framework. The Regulation mandates that all PSPs offering euro credit transfers must also provide instant credit transfers, to be executed within 10 seconds, available 24/7, and interoperable across all EU Member States. The reform seeks to make instant payments the default option for consumers and businesses while embedding robust safeguards against fraud and financial crime.

A central feature of the Regulation, set out in Article 5c, is the mandatory Verification of Payee (VoP) service. PSPs must provide this check free of charge, allowing customers to confirm whether the beneficiary's name matches the IBAN before authorising a transfer. The introduction of VoP marks a key consumer protection measure, expected to significantly reduce losses from impersonation scams. To balance speed with compliance, Article 5d replaces transaction-by-transaction sanctions screening with daily customer-level verification. PSPs may need to update reconciliation, fraud monitoring, and operational resilience systems to cope with instant payments and VoP checks.

NEW: PSD3 / PSR Legislative Package

On 18 June, the Council of the European Union adopted its negotiating mandates on the Payment Services Directive 3 (PSD3) and the PSR, marking a key procedural milestone in the overhaul of EU payment services law and clearing the way for negotiations with the European Parliament.

The legislative package aims to modernise the PSD2 framework by strengthening fraud prevention, harmonising rules across Member States, clarifying the interplay with crypto-asset services, boosting consumer protections, and reducing regulatory fragmentation. Key elements in the Council's text include enhanced anti-fraud provisions, such as IBAN-name checks and stronger information-sharing obligations among PSPs, alongside expanded liability rules and improved consumer redress in cases of impersonation fraud. In November, an agreement reached by Council and Parliament confirmed a strengthened EU-wide fraud and liability framework.

NEW: EU Anti-Fraud Programme II and Calls for Proposals

The European Commission continues to reinforce its commitment to protecting the EU's financial interests through the Union Anti-Fraud Programme (UAFP). As part of the 2021–2027 financing period, the programme allocates funding to national authorities, law enforcement, and related entities to combat fraud, corruption, and irregularities affecting the EU budget.

In March, two calls for proposals were launched, a Technical Assistance call and a Training, Conferences & Studies call. For firms and compliance stakeholders, the calls are a clear signal that anti-fraud efforts are being resourced at scale across the EU scale, with ongoing support for shared tools, investigative capability, and cross-border coordination.

2026 Outlook

NEW: European Commission Launches Review of the EU Anti-Fraud Architecture

In July, EC launched a comprehensive review of the EU Anti-Fraud Architecture. The initiative aims to strengthen the EU's protection against increasingly complex and transnational fraud threats. The review will assess the efficiency and complementarity of all actors involved in the anti-fraud cycle, spanning prevention, detection, investigation, correction, prosecution, and recovery of funds. The Commission noted that effectiveness depends not only on strong rules, but on the ability of regulatory bodies and authorities to work seamlessly together without duplication or fragmentation. The review explicitly seeks to identify opportunities for shared capabilities, improved intelligence flows, and more efficient use of resources. The final output of the review will be presented in a Commission Communication in 2026.

EU Fraud Key Actions

01 Modernise Fraud Detection Frameworks
Prioritise technology-enabled controls such as device intelligence and QA metrics, as supervisors move toward real-time, data-driven fraud detection.

02 Strengthen Cross-Border Fraud Cooperation
Ensure the firm can identify and escalate fraud that spans multiple EU jurisdictions through close collaboration with regulators and intelligence sharing networks.

03 Integrate Fraud into AML Frameworks
Embed fraud typologies into AML systems and TM scenarios as the boundary between fraud and ML continues to narrow.

04 Leverage EU Anti-Fraud Programme II Funding
Take advantage of ongoing EC support for data, analytics, and cross-border fraud prevention through submitting funding proposals for technology enhancements.

05 Enhance Identity Fraud Detection
Reinforce defences against identity manipulation, now a primary enabler of EU fraud schemes by implementing advanced IDV solutions such as liveness detection and biometric matching.

3.4 Sanctions

European Union

New: EBA Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures (EBA/GL/2024/14 and EBA/GL/2024/15):

In December 2024, the EBA published two complementary sets of guidelines establishing a harmonised EU framework for the implementation of Union and national restrictive measures. The Guidelines set detailed expectations for FIs' internal governance, policies, procedures, and controls to ensure effective compliance with sanctions regimes. Both apply from 31 December 2025, marking a major step toward alignment of supervisory expectations across Member States.

- **EBA/GL/2024/14** applies to all firms within the EBA's remit, and requires firms to implement comprehensive, up-to-date internal frameworks covering sanctions compliance, risk assessment, escalation, and reporting. They also mandate the establishment of clear governance structures, ensuring that the management body holds ultimate responsibility for restrictive measures compliance. Firms must conduct exposure assessments to identify vulnerabilities, ensuring that controls are proportionate to their size, nature, and complexity.
- **EBA/GL/2024/15** provides additional requirements for PSPs and CASPs conducting transfers of funds or crypto-assets under Regulation (EU) 2023/1113. These firms must deploy robust, real-time screening systems capable of reliably identifying sanctioned parties, with system parameters calibrated to their specific risk exposure. The Guidelines require PSPs and CASPs to define and update the datasets to be screened, covering both customer and transaction data, and to ensure that all transfers are screened before funds or assets are made available to beneficiaries.

- Firms must establish clear procedures for freezing or suspending assets when a match is identified and ensure that confirmed matches or suspected breaches are reported without delay to national authorities.

By setting a single, consistent standard, the EBA aims to ensure that sanctions implementation is timely, effective, and uniform across the EU, while addressing the technical challenges unique to PSPs and CASPs. The Guidelines represent a significant step in embedding restrictive measures compliance into the EU's broader AML/CFT and financial integrity framework.

Regime and Sector-Specific Sanctions

NEW: EU Lifts Economic Sanctions on Syria

In May, the EU announced the lifting of all economic restrictive measures on Syria with the exception of those based on security grounds, marking a significant shift in the bloc's restrictive measures policy. The decision follows the partial suspension of sanctions earlier in the year and reflects EU ministers' assessment of progress made by the country's transitional government.

While economic sanctions were lifted, the EU confirmed that measures targeting human rights violations, and the Assad regime will remain in force. The European Council's decision to ease restrictions on Syria is explicitly contingent upon sustained and verifiable progress by Syrian authorities. This development illustrates the EU's strategic use of sanctions not merely as punitive measures, but as instruments to encourage political reform, promote transparency, and support long-term stability in post-conflict settings.

UPDATED: EU Sanctions Packages Against Russia

16th Sanctions Package

Adopted in February, the EU's 16th package of restrictive measures against Russia expanded sectoral and individual sanctions in response to the ongoing conflict in Ukraine. The measures introduced additional trade restrictions, tightened controls on dual-use goods and technologies, and broadened the scope of asset freezes. The package also targeted entities accused of facilitating sanctions circumvention, including firms operating through third countries.

17th Sanctions Package

In May 2025, the EU adopted its 17th package, further strengthening restrictions on Russia's financial sector and expanding the framework for countering sanctions evasion. The measures extended prohibitions on providing certain financial and advisory services to Russian entities and introduced new due diligence requirements for firms operating in high-risk third countries suspected of being used to channel goods and funds to Russia. package introduced additional designations targeting individuals and entities linked to Russia's military-industrial complex. The move reinforced the EU's commitment to disrupting access to resources that sustain the war effort.

18th Sanctions Package

By July, the EU agreed on its 18th package of sanctions measures, this time with a sharp focus on enforcement and compliance. The new provisions enhanced information-sharing obligations across Member States, improved mechanisms for tracing frozen assets, and strengthened penalties for breaches. The package also introduced tighter restrictions on sensitive technologies and components with potential military applications. Reflecting the EU's growing emphasis on implementation, this package underscored the importance of consistent enforcement across the Union to close loopholes and ensure sanctions remain effective.

19th Sanctions Package

In October, the EU adopted its 19th package of sanctions against Russia, expanding restrictions on digital assets, maritime activities, and financial infrastructure. The measures introduced new prohibitions on

cryptocurrency and e-money services, a transaction ban on several foreign banks and one crypto firm, and additional vessel designations linked to sanctions evasion. The package also extended the ban on participation in Russia's domestic payment systems, including Measuring Instruments Regulations (MIR) and the Fast Payment System (FPS).

Taken together, these successive packages illustrate a clear evolution in the EU's approach to sanctions against Russia, from expanding prohibitions, to tackling circumvention risks, and now to reinforcing enforcement mechanisms, the strategy is becoming more sophisticated and targeted. Firms must ensure not only their lists, but their approach to sanctions compliance reflects the successive packages and evolving circumvention and evasion risks.

Strategic Evolution

- From expanding prohibitions → to tackling circumvention risks → to reinforcing enforcement
- Increasing focus on emerging evasion channels and digital finance

> **Russia's war economy is sustained by revenues from fossil fuels. We want to cut these revenues. So we are banning imports of Russian LNG into European markets. It is time to turn off the tap.**
>
> Ursula von der Leyen, President of the European Commission

EU Sanctions Timeline: Packages 16–19 Key Focuses (2024–2025)

16th Sanctions Package
February 2025

- Sectoral and individual sanctions
- New trade restrictions
- Dual-use goods and technologies
- Expanded asset freezes
- Facilitating sanctions circumvention via third countries

17th Sanctions Package
May 2025

- Financial sector bans and restrictions
- Due diligence requirements for firms in high-risk third countries
- Military-industrial complex

18th Sanctions Package
July 2025

- Enforcement and compliance
- Information-sharing across Member States
- Tracing frozen assets
- Strengthened penalties for breaches
- Sensitive technologies with military applications

19th Sanctions Package
October 2025

- Digital assets, maritime activities, and financial infrastructure
- Cryptocurrency and e-money services
- Transaction bans
- Designated vessels
- Extended ban on participation in Russia's domestic payment systems

France

UPDATED: French Government Guidance on Economic and Financial Sanctions

In August, the French Government issued updated guidance on compliance with national economic and financial sanctions, consolidating and reframing existing materials to provide a clearer framework for firms. The guidance reaffirmed key obligations under France's asset-freezing and sanctions regimes, including the need to monitor and comply with the official list of designated entities. It further emphasised the need for firms to ensure that all transactions are fully compliant with applicable restrictions, and to promptly declare any suspicions of sanctions circumvention to the relevant authorities. By streamlining these requirements into a single, more coherent document, the French authorities aim to reinforce the effectiveness of the sanctions framework and facilitate stronger compliance across the financial sector.

EU Sanctions Key actions

01

Implement Successive Russia Sanctions Packages

Strengthen sanctions governance, policies, and operational responsiveness as the Russia packages evolve from prohibition to circumvention and enforcement focus.

02

Enhance Detection of Sanctions Circumvention

Document circumvention typologies to identify third-country routing, re-exports, and alternative payment channels used to evade sanctions.

03

Align with National Sanctions Guidance

Ensure EU-level obligations and national guidance (including France) are fully integrated within internal policies and training plans.

3.5 Digital Assets

European Union

NEW: AMF, FMA, and Consob Propose Stronger EU Oversight of Crypto-asset Platforms

In September, three of Europe's leading financial regulators joined forces to call for stronger oversight of crypto markets. The AMF, the Austrian Financial Market Authority (FMA), and Italy's Consob jointly published a paper urging enhanced European-level supervision of crypto-asset markets. The proposal sought to strengthen the EU's regulatory framework following the implementation of MiCA and to address emerging risks linked to the scale and interconnectedness of large crypto platforms.

The authorities recommended that the ESMA be given a greater role in directly supervising major CASPs operating across the Union. They also urged more stringent oversight of global trading platforms that facilitate access for European investors, noting persistent cross-border vulnerabilities and uneven enforcement standards. CASPS should monitor the discussion regarding the proposals closely, ensuring they remain nimble and responsive to a continually evolving regulatory environment and supervisory landscape both across the bloc and internationally.

UPDATED: MiCA Implementation and Supervisory Guidance

The EU's continued regulatory focus on digital assets developed further into implementation in early 2025, as the phased rollout of MiCA Regulation continues to reshape the regulatory landscape for digital assets across the EU.

One of the key developments was ESMA's supervisory briefing on CASP authorisation, which made it clear that no crypto-asset service provider should be considered "low risk" and highlighted key risk factors such as business size, reliance on outsourcing, and underlying business models. Separately, ESMA issued a public statement on Asset-Referenced Tokens (ARTs) and Electronic Money Tokens (EMTs) that are not compliant with MiCA. CASPs operating trading platforms were instructed not to make non-compliant ARTs and EMTs available for trading unless issuers are authorised in the EU, and to cease offering services such as order reception, execution, or crypto-to-crypto exchange in relation to such tokens.

Taken together, these measures reflect the EU's determination to ensure a controlled and consistent transition to MiCA. CASPs should expect heightened supervisory scrutiny to continue as regulators review the resilience of firms' compliance frameworks and the robustness of their governance structures under the new regime.

MiCA Grandfathering Period Timeline

The grandfathering period provides a time-limited window allowing existing CASPs to continue operating under national authorisation regimes before they are required to obtain a MiCA licence. Some jurisdictions provide caveats for application earlier than their designated deadline.

Deadline	Jurisdictions
30 Jun 2025	Latvia, Hungary, Netherlands, Poland, Slovenia, Finland
30 Sept 2025	Sweden
30 Dec 2025	Germany, Ireland, Greece, Spain, Lithuania, Austria, Slovakia, Liechtenstein (EEA), Norway (EEA)
1 Jul 2026	Bulgaria, Czechia, Denmark, Estonia, France, Croatia, Italy, Cyprus, Luxembourg, Malta, Iceland (EEA)

Portugal & Belgian's grandfathering period is still stated as TBA by ESMA.

France

NEW: AMF Position on Implementation of Restrictive Measures

In April, France took another step towards strengthening its sanctions compliance regime. The AMF published Position DOC-2025-02, formally incorporating the EBA guidelines for PSPs and CASPs. The guidelines, issued under Regulation (EU) 2023/1113, establish expectations for firms' internal frameworks to ensure effective implementation of restrictive measures.

The position sets out detailed requirements relating to governance structures, the assessment of corporate exposure to sanctions risks, mechanisms for ensuring the ongoing effectiveness of internal controls, and the provision of staff training. By embedding the EBA's approach into national practice, the AMF underscores the need for consistent alignment between national FI compliance and EU-level requirements. The new rules apply from 30 December 2025, giving firms a defined transition period to review and adapt their governance, policies, and control mechanisms.

2026 Outlook

UPDATED: Monetary and Financial Code – Tax Evasion and Fraud Provisions

On 14 February 2025, France adopted Law No. 2025-127 (Loi des Finances) amending the Monetary and Financial Code (Code Monétaire et Financier). The changes extend tax transparency requirements (including establishing frameworks to identify tax residence information), previously applicable only to FIs, to include CASPs. The new obligations have taken effect from 1 January 2026, marking a significant expansion of France's tax evasion and fraud prevention measures into the digital asset sector and reinforcing the accountability of CASPs in line with broader financial sector standards.

EU Digital Assets Key Actions

01 **Prepare for Enhanced Scrutiny Under MiCA Authorisation**
Position the firm for a smooth transition into the MiCA regime as ESMA and NCAs tighten expectations around governance, operational substance, and documentation.

02 **Implement Reverse Solicitation Guidance**
Prevent unintended or non-compliant solicitation by ensuring all client interactions and onboarding journeys comply with ESMA rules.

03 **Manage Non-Compliant asset-referenced tokens (ARTs) and electronic money tokens (EMTs)**
Mitigate financial, operational, and reputational risk associated with the phase-out of non-MiCA-compliant stablecoins by implementing technical blocks and ongoing due diligence measures.

04 **Strengthen Outsourcing Oversight**
Ensure critical outsourced functions meet MiCA's stringent expectations on governance, accountability, and operational independence through monitoring vendor performance and maintaining robust outsourcing policies.

05 **Integrate Fraud and Financial Crime Risk in Crypto Frameworks**
Conduct robust reviews and internal audits of financial crime controls across crypto operations as regulators intensify focus on ML/TF, sanctions, and fraud risks.

3.6 Conclusion

The EU's financial crime agenda has now entered a decisive phase defined by institutional consolidation, regulatory convergence, and intensifying enforcement. The establishment of AMLA and the operational rollout of MiCA mark structural shifts that are fundamentally reshaping how financial integrity is supervised across the Union. Together, they signal a transition from design to execution.

In 2026, AMLA is expected to assert its role more visibly, setting supervisory priorities, deploying joint supervisory teams, and beginning targeted engagements with firms deemed high-risk across Member States. MiCA will reach its most operational stage as authorisations, outsourcing oversight, and stablecoin compliance reviews provide the first real tests of the framework's robustness. At the same time, sanctions enforcement, particularly related to Russia and high-risk third-country exposure, will continue to tighten, with supervisors placing greater emphasis on circumvention risks, shadow-fleet activity, and consistency of enforcement across the bloc.

The EU's alignment with FATF listings, coupled with political debate over developing a more autonomous EU risk lens, points to further refinement in how external threats are assessed and escalated. Supervisors are also accelerating the adoption of SupTech, leveraging data-driven analytics, AI, and cross-sector information exchange, raising expectations for firms to modernise their own data architecture, monitoring systems, and supervisory-ready reporting capabilities.

France mirrors and accelerates many of these EU-wide trends. Its 2025 reforms extended tax-transparency requirements and due-diligence obligations to CASPs, tightened sanctions implementation, modernised CDD guidance, and expanded obligations beyond traditional FIs to digital asset providers, intermediaries, and high-risk sectors. French supervisors have also signalled heightened intolerance for weak governance, inconsistent documentation, and inadequate monitoring, particularly in fast-growing or technology-driven firms. By aligning closely with EU initiatives under MiCA, TFR, and the emerging AMLA supervisory framework, France positions itself as a jurisdiction that not only adopts Union standards but also pushes for operational rigour and early implementation. This creates a regulatory environment where digital-asset firms, banks, PSPs, and intermediaries must demonstrate the same level of governance maturity, traceability, and escalation procedures expected of established FIs.

Looking ahead, the new AML/CTF legislative package, with many provisions due to take effect in 2027, will complete the shift toward a single, integrated EU financial crime framework. It will solidify AMLA's powers, harmonise CDD standards, unify sanctions implementation expectations, and embed a consistent rulebook across all sectors and jurisdictions. Collectively, these developments reflect a move toward a more harmonised, technologically enabled, and enforcement-led regime, one in which firms must not only meet prescriptive standards but also evidence operational resilience, high-quality data, explainable controls, and a forward-looking approach to emerging risks as supervisory intensity continues to rise.

4 United States

2025 marked a pivotal year for U.S. financial services regulation, with significant recalibration across transparency, enforcement, and digital innovation. The suspension of CTA enforcement for domestic entities signalled a fundamental shift in the U.S. approach to beneficial ownership, narrowing reporting obligations to foreign companies and igniting debate over the future of financial crime prevention. In parallel, the Financial Crimes Enforcement Network (FinCEN) and the Treasury Department moved to reshape the landscape through revised Beneficial Ownership Information guidance, cross-border information-sharing clarifications, and a series of targeted publications designed to keep pressure on high-risk structures and cross-border networks.

Regulators sharpened their focus on threats linked to national-security, issuing detailed advisories and financial trend analyses on ISIS-linked TF, fentanyl-related financial flows, Chinese Money Laundering Networks (CMLN), and bulk cash smuggling tied to Mexico-based transnational criminal organisations. These interventions reinforced a model of intelligence-led supervision, where typology-driven monitoring, outcomes-focused controls, and enhanced law-enforcement engagement are central to expectations for FIs. Alongside this, enforcement bodies such as the Department of Justice recalibrated white-collar crime priorities, emphasising national security, data integrity, and meaningful deterrence through high-impact actions, including landmark asset seizures linked to cryptocurrency scams.

At the same time, the digital asset and payments ecosystem entered a new regulatory phase. The GENIUS Act advanced a federal framework for payment stablecoins, the Digital Asset Market Clarity Act set out oversight for digital commodities, and the House's Anti-Central Bank Digital Currency (CBDC) Surveillance State Act reflected intensified scrutiny of digital currency, privacy, and state control. Federal banking agencies and the Securities Exchange Commission (SEC) signalled a more structured, if still demanding, approach to digital asset oversight, combining clearer supervisory boundaries with continued expectations for robust AML, sanctions, and consumer-protection controls.

Collectively, these developments underscore a U.S. regulatory environment defined by strategic recalibration, technological adaptation, and deeper cross-agency coordination. Looking ahead to 2026, firms face sharper expectations around governance, data quality, and risk-based control design, alongside a clear message that compliance must demonstrate measurable effectiveness, integrating financial crime, sanctions and digital asset risks within a coherent, intelligence-led framework.

What this means in practice

Supervision in 2025 became more data-driven, threat-specific, and operationally intrusive. To meet expectations, firms should ensure:

- Policies, controls, and procedures reflect the latest CTA compliance requirements.
- FinCEN identified threats and typologies are considered and incorporated according on a risk-based approach.
- Record-keeping processes are in line with OFAC's 10-year retention requirement.
- Operationalise digital-asset obligations by mapping GENIUS Act and DAMCA requirements to relevant processes.

The shift is clear: regulators want proof that systems can detect the threats they've flagged, meaning controls must be demonstrably tuned, evidenced in action, and resilient under scrutiny.

4.1 AML/CTF/CPF

Legislation, Regulations, and Guidance

UPDATED: Suspension of the Corporate Transparency Act for U.S. Entities

In March, the U.S. Treasury announced the suspension of enforcement of the CTA for U.S. citizens and domestic reporting companies. The decision halted the imposition of penalties and fines for both current and future CTA rule changes, effectively limiting enforcement to foreign entities. It marked a significant shift in the U.S. approach to corporate transparency and reflects the Trump Administration's broader deregulatory agenda aimed at reducing compliance burdens on U.S. taxpayers and small businesses.

While the change eases reporting obligations for domestic entities, it has sparked debate among transparency advocates, who warn that reduced disclosure may weaken beneficial ownership transparency, one of the primary mechanisms for detecting ML and the misuse of shell companies.

As the revised framework takes effect, firms should review their internal policies on beneficial ownership data collection and reporting, ensuring continued compliance where cross-border structures or foreign affiliates remain in scope.

NEW: House Passed Anti-CBDC Surveillance State Act through Defence Legislation Merger

In September, the U.S. House of Representatives advanced the CBDC Anti-Surveillance State Act by merging it into the National Defence Authorisation Act, significantly increasing the likelihood of Senate consideration. While the bill primarily limits the Federal Reserve's authority to issue or operate a retail CBDC, it also carries important implications for FCC. By restricting the development of a government-managed digital currency, the legislation effectively preserves the current decentralised ecosystem in which FIs remain the primary gatekeepers for AML/CFT and sanctions controls in digital payments.

FINCEN AML /CTF /CPF Publications

Date	Title	Key Points	Impacts for Firms
26/02/2025	NEW: FinCEN FAQs on the Beneficial Ownership Information Interim Final Rule	• FinCEN's Interim Final Rule removes BOI reporting requirements for U.S. companies and U.S. persons. • Domestic entities are now formally exempt from BOI reporting. • Only foreign entities registered to do business in the U.S. must report BOI unless exempt.	• Update BOI/CTA policies to reflect the exemption for domestic entities. • Ensure onboarding processes identify foreign entities requiring BOI reporting. • Refresh client communications and disclosures accordingly.

Date	Title	Key Points	Impacts for Firms
31/03/2025	NEW: FinCEN Alert on Bulk Cash Smuggling and Repatriation by Mexico-Based Transnational Criminal Organisations	• FinCEN issued an alert on bulk cash smuggling and repatriation by Mexico-based TCOs. • Identified typologies include cross-border cash transport, commingling through exchange houses, and front companies masking deposits. • Reinforces SAR obligations and references specific terminology for reporting.	• Integrate FinCEN typologies into monitoring for cash-intensive and cross-border activity. • Enhance due diligence on currency exchange businesses and other high-risk cash operators. • Ensure SARs referencing relevant red flags use FinCEN's specified key terms.
04/01/20…	NEW: FinCEN Advisory on ISIS-Linked Terrorist Financing	• FinCEN issued an advisory on detecting ISIS-linked TF. • Highlights misuse of NPOs, Informal Value Transfer Systems (IVTS), digital assets, and front companies. • Notes ISIS networks remain active across West Africa, the Levant, and Central Asia.	• Update TF risk assessments to include patterns linked to ISIS financing. • Incorporate FinCEN red flags into monitoring and screening rules. • Strengthen controls around NPOs, digital assets, and high-risk jurisdictions.
04/09/20…	NEW: FinCEN Issued Analysis on Fentanyl-Related Financial Threats	• FinCEN released an analysis of fentanyl-related financial activity. • Identified patterns include bulk precursor purchases, misuse of import/export firms, and small-value transfers inconsistent with customer profiles. • Provides red flags based on BSA reporting from 2021–2024.	• Add fentanyl-related red flags to monitoring rules and alert logic. • Review customers dealing in chemicals, logistics, or import/export for elevated risk. • Ensure SARs reference relevant fentanyl typologies where applicable.

Date	Title	Key Points	Impacts for Firms
28/08/20…	NEW: FinCEN Issued Advisory and Financial Trend Analysis on Chinese Money Laundering Networks	• FinCEN issued an Advisory and Financial Trend Analysis on Chinese Money Laundering Networks (CMLNs). • CMLNs were linked to $312 billion in suspicious transactions (2020–2024) and support narcotics trafficking, fraud, human trafficking, and human smuggling. • FinCEN highlighted CMLNs' role in laundering proceeds for Mexico-based drug cartels, including FTO-designated groups. • Publications provide red flags and typologies involving funnel accounts, bulk cash, TBML, and cross-border remittances.	• Integrate CMLN-related red flags into monitoring, especially for funnel accounts and cross-border transfers. • Review exposure to high-risk intermediaries, import/export firms, and cash-intensive businesses. • Strengthen SAR narratives referencing FinCEN's CMLN typologies and terminology. • Refresh TF, drug-trade, and organised-crime risk assessments to include CMLN-linked activity
05/09/20…	NEW: FinCEN Guidance on Cross-Border Information Sharing	• FinCEN issued guidance encouraging U.S. FIs to voluntarily share cross-border information with regulated foreign firms. • The aim is to strengthen joint efforts against ML, TF, narcotics trafficking, FTO activity, and major fraud. • FinCEN clarified that SARs and SAR-related information cannot be shared, but most other relevant financial crime information can be shared internationally.	• Review and update information-sharing policies to reflect what can be shared cross-border under the BSA. • Enhance coordination between U.S. and non-U.S. compliance teams to support intelligence-driven investigations. • Train staff on permissible vs. prohibited information sharing, especially regarding SAR confidentiality.

US AML Key Actions

01

Embed Proportionate Risk-Based Approaches

Test whether controls match exposure by performing proportionality assessments against FinCEN/Treasury expectations, documenting gaps and remediation plans.

02

Enhance Detection of Transnational Financial Crime

Map FinCEN typologies (ISIS, fentanyl, CMLNs, bulk cash) to monitoring rules and case-handling procedures, evidencing updates in control change logs.

03

Evolve Suspicious Activity Monitoring and Reporting

Embed explainability into analytics models and maintain audit-ready logs demonstrating how alerts were generated and escalated.

04

Enhance Governance, Accountability, and Data Quality

Upgrade BSA reporting processes, implement data-quality controls, and maintain exception logs showing completeness, timeliness, and accuracy issues.

4.2 Enforcement

NEW: Department of Justice Outlined Updated Priorities for White-Collar Crime Enforcement

In May, the U.S. Department of Justice issued updated guidance on white-collar crime enforcement, signalling a sharper focus on cases with national security implications, including sanctions violations, tariff evasion, fraud involving government programmes, and corporate links to transnational criminal or terrorist organisations. For firms, the memo reinforces that prosecutors will prioritise swift action where misconduct creates systemic risk or significant public harm, while also rewarding voluntary self-disclosure, cooperation, and timely remediation. The shift underscores the importance for firms to maintain strong sanctions controls, robust fraud and corruption monitoring, and clear escalation pathways, as well as to document compliance decisions that demonstrate good-faith efforts to prevent and respond to misconduct. The DOJ's guidance can be viewed as an indicator of rising expectations around corporate accountability and a roadmap for mitigating enforcement exposure.

NEW: FinCEN Published Its Fiscal Year 2024 in Review Report

In June, FinCEN published its Fiscal Year 2024 (FY24) in Review Report, highlighting the agency's operational achievements and the ongoing impact of BSA reporting in supporting law enforcement investigations.

FinCEN reported that 32% of cases within the Federal Bureau of Investigation's (FBI) Complex Financial Crime Program were linked to SARs and Currency Transaction Reports (CTRs), demonstrating the critical value of FIs' reporting in identifying and disrupting criminal activity. During FY24, Homeland Security Investigations (HSI) personnel conducted approximately 290,000 BSA-related queries, reflecting the growing reliance on FinCEN's data by federal investigative agencies. FinCEN also recorded the receipt of approximately 4.7 million SARs and 20.5 million CTRs during the

fiscal year, illustrating both the scale and operational reach of the U.S. financial intelligence framework.

NEW: DOJ Seized $225 Million Linked to Cryptocurrency Confidence Scams

In June, the DOJ announced the seizure of approximately $225 million in assets connected to cryptocurrency confidence scams. According to federal prosecutors, victims were manipulated into establishing fraudulent online relationships via messaging platforms and social media before being coerced into investing in fake cryptocurrency trading websites. Funds were subsequently diverted through hundreds of accounts across multiple virtual asset service providers (VASPs) and foreign exchanges, making the recovery effort one of the largest digital asset seizures to date related to online financial exploitation. The seizure demonstrated the U.S. government's ongoing commitment to targeting illicit cryptocurrency activity, protecting retail investors, and disrupting cross-border financial crime networks.

US Enforcement Key Actions

01

Enhance Corporate Accountability and Cooperation

With regulators prioritising self-disclosure and organisational culture resource and oversee whistleblower and ethics programmes, ensuring reports are independently triaged and linked to updated misconduct-risk metrics.

02

Address Digital Asset and Transnational Crime Risks

Deploy blockchain analytics and cross-border trace tools; document risk scoring logic and investigative case files.

03

Reinforce Sanctions and National Security Compliance

Update sanctions policies for OFAC's ten-year recordkeeping rule and national-security priorities; ensure evidence logs capture all screening and blocking decisions.

04

Advance Data Integrity and Documentation Standards

Enhance digital-evidence retention and traceability by testing metadata integrity, backup processes, and investigation-file completeness.

4.3 Sanctions

Legislation

NEW: OFAC Finalised Rule Extending Recordkeeping Requirements to Ten Years

In March, OFAC finalised a rule extending certain sanctions-related recordkeeping requirements under the Reporting, Procedures and Penalties Regulations (RPPR) from five years to ten years. The final rule adopted OFAC's earlier interim final rule, bringing U.S. sanctions recordkeeping obligations into alignment with the extended statute of limitations for violations of the International Emergency Economic Powers Act (IEEPA) and the Trading with the Enemy Act (TWEA).

The amendment, which took effect on 21 March 2025, implemented updates introduced by the 21st Century Peace Through Strength Act, enacted in April 2024, which lengthened the federal statute of limitations for sanctions-related violations from five to ten years. By extending the record retention period, OFAC aimed to enhance enforcement capabilities and ensure that documentation is available throughout the full period in which potential violations may be prosecuted.

The change amended 31 CFR Part 501, requiring FIs, businesses, and individuals subject to OFAC jurisdiction to retain all relevant sanctions compliance records, including transaction data, internal communications, due diligence findings, and blocked property reports, for ten years from the date of the transaction or activity.

Regime and Sector-Specific Sanctions

NEW: OFAC Issued General License 25 Lifting Sanctions on Syria

On 23 May, OFAC issued General License 25, providing immediate relief from U.S. sanctions on Syria. The measure followed President Trump's announcement of a full cessation of sanctions under the administration's "America First" foreign policy strategy, which aimed to enable new investment and economic engagement in Syria as part of a broader U.S. initiative to support the country's post-conflict recovery and political transition.

The licence authorised a wide range of previously prohibited activities under the Syrian Sanctions Regulations (31 CFR Part 542), including new investment, financial services, and trade in petroleum products. It explicitly excluded transactions that could directly or indirectly benefit Russia, Iran, North Korea, or designated terrorist organisations, maintaining targeted prohibitions consistent with U.S. national security objectives. In parallel, the U.S. Department of State issued a waiver under the Caesar Syria Civilian Protection Act (Caesar Act) to facilitate international engagement and reconstruction assistance, allowing global partners to participate in Syria's economic stabilisation without breaching U.S. law.

The issuance of General License 25 reflected a recalibration of U.S. strategy from broad economic isolation to selective re-engagement, aimed at countering regional adversaries' influence while supporting private-sector investment and humanitarian development.

NEW: U.S. Expands Sanctions on Russian Oil Majors While Granting Temporary Waiver for Lukoil Retail Network

In October, the U.S. Department of the Treasury intensified economic pressure on Moscow by designating Rosneft and Lukoil, Russia's two largest oil producers, along with numerous subsidiaries, under Executive Order 14024. Citing Russia's lack of engagement in efforts toward a Ukraine ceasefire, the sanctions are intended to degrade the Kremlin's revenue from energy exports, constraining its ability to fund ongoing military operations.

Complementing these measures, OFAC issued a targeted waiver on 4 December 2025 permitting continued operations of Lukoil-branded fuel stations located outside Russia until 29 April 2026. The waiver covers roughly 2,000 stations across Europe, Central Asia, the Middle East, the Americas, and nearly 200 sites

in the U.S, with bans preventing flow of money back into Russia remaining in place. The extension delays previously mandated wind-down deadlines and aims to prevent abrupt fuel-supply disruptions while host countries and operators organise the divestment or transition of these assets.

US Sanctions Key Actions

01

Reinforce Sanctions Governance and Oversight
Update sanctions policies to incorporate OFAC's 10-year RPPR recordkeeping rule and GL25 permissions/exclusions.

02

Embed Sanctions Exposure Into EWRAs
Integrate sanctions exposure, including Syria re-engagement and higher-risk corridors, into enterprise-wide risk assessments, documenting updated risk factors.

03

Strengthen Cross-Border and Foreign Policy Compliance
Conduct EDD for activities involving Syria, Iran, or other high-risk jurisdictions, documenting independent reviews and licensing decisions.

04

Enhance Recordkeeping and Documentation Standards
Ensure systems support long-term, tamper-proof storage (e.g., immutable logs) and rapid retrieval for regulatory inquiries.

05

Advance Intelligence Sharing and Collaboration
Disseminate updated typologies internally and incorporate them into screening rules, sanctions playbooks, and escalation criteria.

4.4 Digital Assets

Legislation

NEW: GENIUS Act Established Federal Framework for Stablecoin Regulation

The GENIUS Act (S.1582) establishes the first comprehensive federal framework for regulating payment stablecoins in the U.S., restricting issuance to authorised entities and requiring strict 1:1 high-quality liquid reserves, clear redemption rights, and enhanced governance and disclosure standards. By confirming that permitted stablecoin issuers are "financial institutions" under the Bank Secrecy Act, the Act brings these entities squarely within federal AML/CTF expectations, mandating risk assessments, CDD, monitoring, record-keeping, and sanctions compliance comparable to traditional FIs. The framework also clarifies regulatory boundaries between the SEC, Commodity Futures Trading Commission (CFTC), and banking regulators, and applies to certain foreign issuers operating in U.S. markets.

For firms, these Acts require updating AML/CFT controls, enhancing governance and reserve management, and preparing for structured supervisory engagement across stablecoin and digital commodity activities. Treasury's 2025 Request for Comment on compliance technologies (AI, digital ID, Application Programming Interfaces (APIs), blockchain analytics) indicates an expectation that firms will invest in technology-enabled detection and monitoring, ahead of rulemaking that will operationalise these standards.

NEW: House Passed the Digital Asset Market Clarity Act to Regulate Digital Commodities

The U.S. House of Representatives passed the Digital Asset Market Clarity Act of 2025, introducing a federal framework that assigns the CFTC primary oversight of digital commodities and the intermediaries supporting their trading. While the Act aims to clarify jurisdictional boundaries across U.S. regulators, its most consequential elements for financial crime relate to the extension of Bank Secrecy Act and AML obligations to digital commodity exchanges, brokers, and dealers. Banks and intermediaries must implement robust risk assessment, CDD, transaction monitoring, and oversight of third-party custody to mitigate ML, sanctions, fraud, and consumer protection risks in digital assets. The Act also establishes eligibility and disclosure standards that enhance traceability and transparency, key tools for detecting illicit activity on blockchain networks.

Taken together, the Act complements the GENIUS stablecoin framework by embedding clearer federal expectations for AML/CTF controls across a broader set of digital-asset business models, reinforcing coordinated supervision between the CFTC, SEC, and Treasury.

Government Publications

NEW: Federal Reserve, FDIC, and OCC Issued Joint Statement on Crypto-asset Safekeeping by Banks

U.S. banking regulators, the Federal Reserve, Federal Deposit Insurance Corporation (FDIC), and Office of the Comptroller of the Currency (OCC), issued a joint statement clarifying how existing regulatory expectations apply to banks offering crypto-asset safekeeping services. While primarily focused on operational and governance risks, the guidance reinforces key FCC obligations: banks must conduct comprehensive risk assessments before launching custody services, ensure strong controls around CDD and transaction integrity, and maintain oversight of third-party providers involved in wallet management or key custody. Firms are expected to evidence the ability to identify and mitigate ML, sanctions, and fraud risks associated with digital assets, supported by appropriate internal controls, audit mechanisms, and ongoing monitoring. The statement forms part of broader interagency efforts to ensure that bank participation in digital-asset markets occurs within a controlled, compliance-focused framework.

NEW: FinCEN Issued Notice on Risks of Convertible Virtual Currency (CVC) Kiosks

In August, FinCEN issued a notice warning FIs about the illicit finance and consumer protection risks associated with CVC kiosks, also known as Crypto ATMs. FinCEN highlighted that risks were elevated when CVC kiosk operators failed to comply with BSA registration, reporting, and due diligence requirements. The notice detailed typologies linking CVC kiosk misuse to fraud, cybercrime, and drug trafficking, all of which are designated as national AML/CFT priorities under FinCEN's strategic framework.
The notice provided a range of red flag indicators, including patterns of small-value, rapid transactions by unrelated individuals, repeated deposits to the same wallet address, and transfers involving elderly or vulnerable customers who had been deceived through relationship or investment scams. FinCEN emphasised that FIs should give special attention to BSA reporting obligations, particularly in cases involving fraud targeting older adults.

NEW: SEC Signals Shift in Digital Asset Enforcement Approach

The SEC signalled a more calibrated approach to digital asset enforcement in 2025, with the dismissal of Civil Enforcement Action Against, Binance, Coinbase, Kraken, and Ripple and focusing instead on areas with clearer investor-protection and market-integrity risks. For FCC teams, the shift suggests a regulatory environment where governance, disclosure quality, and control effectiveness will carry greater weight than broad assertions about token classification. The publication of no-action letters, covering select stablecoin structures, tokenised instruments, and blockchain-based settlement tools, highlights an expectation for firms to implement strong risk management, transparency, and consumer-protection standards. The SEC's objectives and approaches to enforcement will offer firms a clearer compliance pathway as federal digital-asset legislation advances.

US Digital Assets Key Actions

01

Establish Robust Governance for Digital Asset Compliance

Map supervisory obligations across federal agencies for stablecoins, digital commodities, custody services, and tokenised products; maintain an updated, evolving obligation register.

02

Strengthen AML/CFT and Sanctions Controls in Digital Ecosystems

Apply FinCEN digital-asset red flags to monitoring and SAR reporting, especially for elderly-targeted scams, rapid small-value transfers, and kiosk-linked typologies.

03

Enhance Regulatory Engagement and Policy Participation

Participate in cross-sector working groups to influence proportionate, innovation-friendly frameworks and share typology intelligence with peers and regulators.

04

Promote Consumer Protection and Market Integrity

Deliver customer education covering scam indicators, stablecoin redemption rights, and custody risks, prioritising channels where older or vulnerable customers interact.

4.5 Conclusion

U.S regulatory updates in 2025 had common themes of inter-government coordination, technological adaptation, and strategic recalibration. The suspension and narrowing of CTA enforcement for domestic entities sat alongside intensified, typology-led action on fentanyl financing, CMLNs, ISIS-linked activity, bulk cash and CVC kiosks, underscoring that while some burdens were eased, expectations around outcomes and risk management remained and increased.

In parallel, the U.S advanced a new generation of digital asset legislation and guidance. The GENIUS Act and the Digital Asset Market Clarity Act began to anchor stablecoins and digital commodities within prudential, BSA-aligned frameworks, while the Anti-CBDC Surveillance State Act and a more calibrated SEC enforcement stance reflected heightened supervisory expectations. Developments reinforced a common theme: innovation is not being curtailed, but it must sit on top of robust governance, reserves, surveillance, and consumer safeguards.

What emerges is a regulatory environment increasingly defined by proportionality and intelligence-led supervision. Firms are expected not merely to comply on paper, but to evidence active control, measurable effectiveness, and responsible innovation across AML/CTF/CPF, enforcement, fraud, sanctions, and digital assets.

Looking ahead to 2026, U.S. policy will focus on deepening public–private collaboration, operationalising the new digital asset frameworks, and rigorous supervision and enforcement. For FIs, the central challenge is to maintain agility and trust: proving that as enforcement sharpens and innovation accelerates, controls remain explainable, evidenced, and operationally resilient.

5 Singapore

Singapore's financial crime landscape in 2025 was defined by a decisive shift toward stronger regulatory foundations, firmer supervisory expectations, and heightened accountability across the financial sector. The Monetary Authority of Singapore (MAS) issued extensive updates to its AML/CFT/CPF Notices and Guidelines that took effect from mid-year. These revisions clarified and strengthened requirements on CDD, BO identification, Source of Wealth (SoW) and Source of Funds (SoF) corroboration, PF risk assessment, and STR reporting timelines, while ensuring alignment with evolving FATF standards. Industry guidance continued to mature in parallel, with the AML/CFT Industry Partnership (ACIP's) best practices on establishing SoW reinforcing the need for consistent, risk-proportionate due diligence across private, corporate, and retail banking.

The regulatory reforms were paired with one of the most active enforcement periods Singapore has seen. MAS imposed significant penalties on banks, capital markets intermediaries, trust companies, and major payment firms for AML/CFT failings, including cases tied to the 2023 ML investigation. Expanded investigative powers, enhanced prohibition order regimes, and supervisory scrutiny of senior individuals highlighted MAS's sharpened focus on governance, escalation discipline, and the effectiveness of first- and second-line controls. These outcomes are already driving widespread remediation efforts and informing MAS's planned thematic reviews into 2026.

In parallel, Singapore continued to bolster its national response to rising fraud and cyber-enabled scams. Joint advisories issued by MAS, Singapore Police Force (SPF), and Cyber Security Agency of Singapore (CSA) responded to a sharp escalation in phishing and mobile-wallet–enabled fraud, while SPF's Scam and Cybercrime Report underscored ongoing vulnerabilities in consumer behaviour, digital payment channels, and real-time authentication processes. FIs are increasingly expected to integrate behavioural analytics, multi-factor authentication safeguards, and enhanced customer education into their fraud risk management frameworks.

Collectively, these developments reflect a regulatory environment that is increasingly rigorous, data-driven, and focused on implementation quality. Singapore's approach continues to balance digital innovation with system integrity, reinforcing the need for firms to adopt technology-enabled, risk-sensitive controls and strong governance across AML/CFT/CPF, fraud, and digital asset activities.

What this means in practice

Firms should be prepared to demonstrate that processes operate reliably under real conditions.

In practice, this means:

- Verify end-to-end CDD and SoW/SoF
- Ensure controls are operating effectively, throughout the customer journey
- Perform focused quality reviews on recent STRs to understand risk
- Stress-test fraud and digital-payments controls
- Document decision-making clearly to ensure traceability

In essence, firms should anticipate deeper, data-led supervision where the effectiveness of controls is tested, validated, and expected to hold up operationally.

5.1 AML/CTF/CPF

UPDATED: MAS AML/CTF Notices and Guidelines

In April, MAS issued a consultation proposing extensive amendments to its AML/CFT Notices and related Guidelines for FIs and Variable Capital Companies (VCCs). The consultation reflected the regulator's objective to strengthen Singapore's financial crime prevention framework and align domestic regulations with evolving FATF standards. Changes were subsequently implemented on 30 June 2025.

Notices

The following sectoral MAS AML/CTF Notices & Guidelines to Notices were amended:

Sector	AML/CTF Notices	Guidelines to Notices
Banks	· MAS Notice 626 – Prevention of Money Laundering and Countering the Financing of Terrorism – Banks	· Guidelines to MAS Notice 626 – Prevention of Money Laundering and Countering the Financing of Terrorism – Banks
Direct Life Insurers	· MAS Notice 314 – Prevention of Money Laundering and Countering the Financing of Terrorism – Direct Life Insurers	· Guidelines to MAS Notice 314 – Prevention of Money Laundering and Countering the Financing of Terrorism – Direct Life Insurers
Digital Token Service Providers	· MAS Notice PS-N02 – Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Digital Payment Token Service) · MAS Notice FSM-N27 – Prevention of Money Laundering and Countering the Financing of Terrorism – Digital Token Service Providers	· Guidelines to MAS Notice PS-N02 – Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Digital Payment Token Service)
Credit Card or Charge Card Licensees	· MAS Notice 626A – Prevention of Money Laundering and Countering the Financing of Terrorism – Credit Card or Charge Card Licensees	· Guidelines to MAS Notice 626A – Prevention of Money Laundering and Countering the Financing of Terrorism – Credit Card or Charge Card Licensees

Sector	AML/CTF Notices	Guidelines to Notices
Finance Companies	· MAS Notice 824 – Prevention of Money Laundering and Countering the Financing of Terrorism – Finance Companies	· Guidelines to MAS Notice 824 – Prevention of Money Laundering and Countering the Financing of Terrorism – Finance Companies
Merchant Banks	· MAS Notice 1014 – Prevention of Money Laundering and Countering the Financing of Terrorism – Merchant Banks	· Guidelines to MAS Notice 1014 – Prevention of Money Laundering and Countering the Financing of Terrorism – Merchant Banks
Financial Advisers	· MAS Notice FAA-N06 – Prevention of Money Laundering and Countering the Financing of Terrorism – Financial Advisers	· Guidelines to MAS Notice FAA-N06 – Prevention of Money Laundering and Countering the Financing of Terrorism – Financial Advisers
Payment Service Licensees	· MAS Notice PS-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services)	· Guidelines to MAS Notice PS-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Holders of Payment Services Licence (Specified Payment Services)
Approved Exchanges & Recognised Market Operators	· MAS Notice SFA02-N05 – Prevention of Money Laundering and Countering the Financing of Terrorism – Approved Exchanges and Recognised Market Operators	· Guidelines to MAS Notice SFA02-N05 – Prevention of Money Laundering and Countering the Financing of Terrorism – Approved Exchanges and Recognised Market Operators
Central Depository System	· MAS Notice SFA03AA-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – The Depository	· Guidelines to MAS Notice SFA03AA-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – The Depository
Capital Market Intermediaries	· MAS Notice SFA04-N02 – Prevention of Money Laundering and Countering the Financing of Terrorism – Capital Market Intermediaries	· Guidelines to MAS Notice SFA04-N02 – Prevention of Money Laundering and Countering the Financing of Terrorism – Capital Market Intermediaries
Approved Trustees	· MAS Notice SFA13-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Approved Trustees	· Guidelines to MAS Notice SFA13-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Approved Trustees

Sector	AML/CTF Notices	Guidelines to Notices
Approved Trustees	· MAS Notice SFA13-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Approved Trustees	· Guidelines to MAS Notice SFA13-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Approved Trustees
Trust Companies	· MAS Notice TCA-N03 – Prevention of Money Laundering and Countering the Financing of Terrorism – Trust Companies	· Guidelines to MAS Notice TCA-N03 – Prevention of Money Laundering and Countering the Financing of Terrorism – Trust Companies
Variable Capital Companies	· MAS Notice VCC-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Variable Capital Companies	· Guidelines to MAS Notice VCC-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – Variable Capital Companies
FIs dealing in Precious Stones, Precious Metals, & Precious Products	· MAS Notice PSM-N01 – Prevention of Money Laundering and Countering the Financing of Terrorism – FIs dealing in Precious Stones, Precious Metals and Precious Products	

Amendments to MAS Notices included	Amendments to MAS Guidelines to Notices included
• Clarifications that ML includes PF, and that the ML/TF risk assessments carried out by FIs and VCCs must include PF risk assessments. • MAS Notice TCA-N03 was aligned with the Trustees Act 1967 and related legislative changes that had originally resulted from the revised FATF Recommendation 25.	• Requirements for STRs to be filed within five working days once suspicion is established, and within one day for sanctions-related cases, with further guidance on the 'establishment of suspicion'. • Expectations on sanctions screening solutions and vendor assessments . • SoW and SoF clarifications, also highlighting that firms shouldn't take a 'one-size-fits-all' approach to establishing SoW. • Clarified requirements on identifying beneficial owners, including the requirement to identify legal persons/arrangements in an ownership or control structure .

MAS's updated Notices and Guidelines drive firms to operationalise more consistent, technology-enabled, and risk-sensitive controls, signalling the Authority's intent to maintain a harmonised, FATF-aligned framework that is both resilient and forward-looking.

NEW: ACIP Best Practices Paper on Establishing Sources of Wealth

In May, ACIP Legal Persons and Arrangements Working Group published a best practices paper aimed at helping FIs strengthen their approach to establishing customers' SoW.

The paper builds on guidance previously issued by MAS, including Circular AMLD 08/2024 and the October 2024 Information Paper on AML/CFT Inspection Findings, both of which underscored the importance of robust verification of wealth provenance, particularly in the context of EDD for high-risk clients such as PEPs. The ACIP paper provides practical recommendations and illustrative case studies to support FIs in adopting a risk-proportionate and reasonable approach to SoW assessment.

FIs should implement risk-proportionate SoW verification across private, corporate, and retail banking, ensuring assets and their origin are fully understood to inform accurate risk profiling. For example, updating CDD processes and applying the "same risk, same control" principle consistently across client segments.

Singapore AML Key Actions

01

Implement Revised AML/CFT Frameworks
Embed the extensive 2025 MAS AML/CFT updates across governance, controls, and reporting processes to ensure full alignment with revised regulatory expectations.

02

Strengthen CDD and SoW Verification
Reinforce end-to-end due diligence practices by applying MAS and ACIP expectations on SoW verification, especially for higher-risk clients and products.

03

Leverage Technology and Data for Financial Crime Prevention
Accelerate the adoption of analytics-led, explainable technology to strengthen detection, reporting, and real-time response to financial crime risks.

5.2 Enforcement

Regulatory Publications

UPDATED:MAS Enforcement Report 2023–2024

In April, MAS released its Enforcement Report covering the period from 1 July 2023 to 31 December 2024, providing a comprehensive overview of enforcement actions, case outcomes, and regulatory priorities. The report reaffirmed MAS's core enforcement principles of deterrence, proportionality, and transparency.

During the reporting period:

- Legislative changes expanded MAS's investigative and enforcement powers by facilitating domestic and international evidence sharing, and extending prohibition orders to include individuals and roles essential to FIs' integrity, even if outside direct regulatory oversight,
- 2 capital markets services licensees were fined $4.4 million for AML/CFT breaches, and
- ML-related control breaches were a key focus area, including inadequate processes and failures to identify SoW/SoF for high-risk customers.

NEW: MAS and HKMA Sign MoU to Enhance Banking Supervisory Cooperation

In September, MAS and the Hong Kong Monetary Authority (HKMA) signed an MoU to strengthen bilateral banking supervisory cooperation, formalising their long-standing partnership and establishing a structured framework for information exchange, mutual assistance, and the sharing of supervisory best practices. The agreement reflects the growing cross-border activity between banks operating in both financial centres and aims to improve oversight through timely communication and coordinated responses to prudential and governance risks. The initiative marks a significant step toward regional supervisory convergence and financial stability, aligning with broader trends in cross-border regulatory collaboration across Asia.

Penalty Actions

NEW: MAS Imposes S$960,000 in Penalties on Major Payment Institutions for AML/CFT Breaches

In June, MAS announced the imposition of composition penalties totalling S$960,000 on five licensed major payment institutions (MPIs) for multiple breaches of AML/CFT requirements. The sanctioned entities were found to have significant control weaknesses in their compliance frameworks, resulting in failures to meet core regulatory obligations. MAS's investigations identified deficiencies across several key areas, including CDD, wire transfer information, screening of customers and beneficial owners, and the documentation of authority to act on customer accounts. These lapses, the Authority noted, exposed the firms to elevated ML/TF risks and undermined the transparency of cross-border payment flows.

The enforcement action reflects MAS's ongoing supervisory focus on the payments sector, a rapidly growing and high-risk segment of Singapore's financial ecosystem. The Authority also indicated that it will issue an information paper in early 2026 to highlight common deficiencies and clarify supervisory expectations for AML/CFT compliance among PSPs.

NEW: MAS Takes Regulatory Action Against Nine FIs for AML Breaches

In July, MAS announced regulatory actions against nine FIs and 16 individuals for breaches of AML requirements linked to the major 2023 ML case, one of Singapore's largest financial crime investigations to date. A total of S$27.45 million in composition penalties was imposed on the firms involved, which included several prominent banks. MAS identified a range of compliance failures, including inadequate customer risk assessments, insufficient corroboration of sources of wealth, weaknesses in TM, and deficiencies in post–STR follow-up.

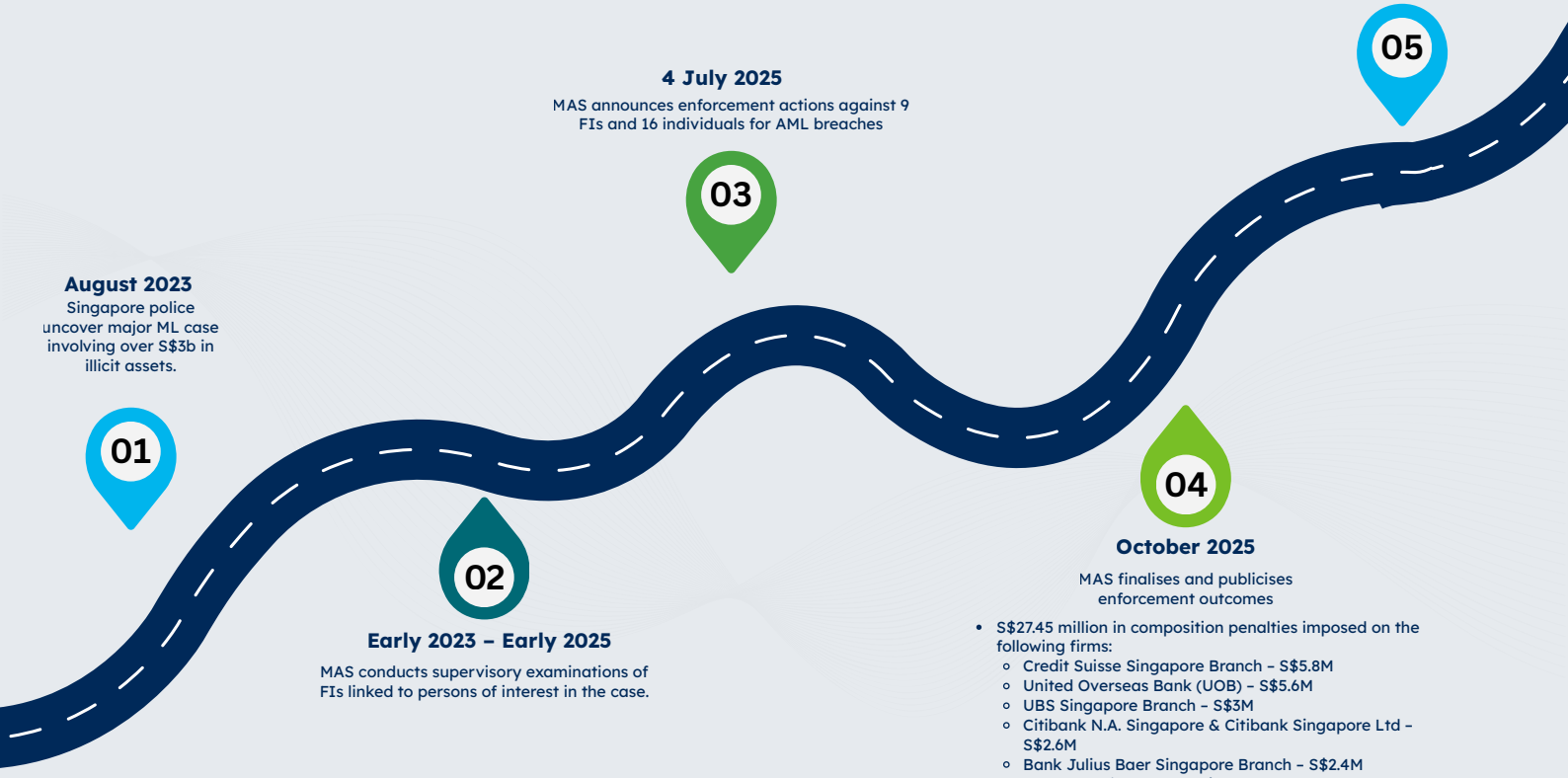
In addition to financial penalties, MAS issued Prohibition Orders (POs) of up to six years against senior individuals formerly associated

with one of the firms, barring them from performing regulated activities.

Further reprimands were issued to executives at 2 others for failures in governance and oversight. MAS emphasised that effective management of financial crime risk begins at the front line and reiterated the expectation for firms to uphold rigorous standards of due diligence, monitoring, and escalation.

The enforcement action marked one of the most significant supervisory responses in recent years, both in scale and industry impact. The case prompted extensive reviews of AML frameworks across Singapore's banking and trust sectors, driving a renewed focus on governance, accountability, and the practical application of MAS's supervisory expectations and industry best practices. The Authority noted that it would continue to leverage lessons from this case to inform future thematic inspections and sectoral guidance in 2026.

MAS Enforcement Timeline



- S$27.45 million in composition penalties imposed on the following firms:
  - Credit Suisse Singapore Branch – S$5.8M
  - United Overseas Bank (UOB) – S$5.6M
  - UBS Singapore Branch – S$3M
  - Citibank N.A. Singapore & Citibank Singapore Ltd – S$2.6M
  - Bank Julius Baer Singapore Branch – S$2.4M
  - LGT Bank Singapore – S$1M
  - UOB Kay Hian Private Ltd – S$2.85M
  - Blue Ocean Invest Pte Ltd – S$2.4M
  - Trident Trust Company Singapore – S$1.8M

Singapore Enforcement Key Actions

01

Strengthen Governance and Accountability Frameworks

Review and approve an updated AML accountability and oversight framework that clearly maps control ownership, escalation obligations, and governance enhancements required in light of recent MAS enforcement themes.

02

Embed Lessons from Recent Enforcement Outcomes

Conduct targeted reviews of high-risk areas cited in MAS actions, including SoW corroboration, TM alert handling, and sanctions escalations, issuing formal findings and remediation timelines.

03

Promote a Culture of Deterrence and Ethical Conduct

Update mandatory training programmes with anonymised MAS case studies to reinforce expectations for escalation, documentation quality, and monitoring discipline across all front-line and control staff.

5.2 Fraud

NEW: Joint Advisory on Unauthorised Contactless Card Transactions

In February, the SPF, CSA, and MAS issued a joint advisory after a surge in unauthorised contactless card transactions, with 656 reported cases and over S$1.2 million in losses between October and December 2024. Criminals used phishing sites to steal card details and one-time passwords (OTPs), enabling them to link victims' cards to mobile wallets and make in-person contactless payments. The advisory highlighted the need for stronger authentication, enhanced monitoring of wallet linkages, and improved public education to mitigate rising scam risks in Singapore's increasingly digital payment landscape.

Scams Identified

- Phishing sites harvesting card details by mimicking banks and merchants
- OTP harvesting to enable wallet enrolment
- Fraudulent mobile wallet linkage using stolen credentials
- Unauthorised contactless payments made at physical retail outlets

Actions for Firms

- Strengthen authentication and verification for mobile wallet provisioning
- Enhance monitoring to detect suspicious or repeated wallet-linkage attempts
- Improve fraud-response processes to rapidly block compromised cards or wallets
- Increase customer education on phishing risks and secure card-handling practices

UPDATED: Singapore Police Force Scam and Cybercrime Report 2024

In February, the SPF released its 2024 Scam and Cybercrime Report, showing a 10.8% rise in cases to 55,810 and total losses reaching S$1.1 billion, despite S$182 million being successfully recovered. While some scam types declined, sharp increases in e-commerce, phishing, and investment scams demonstrated the continued evolution of cyber-enabled fraud. Notably, self-effected scams accounted for over 82% of cases, underscoring ongoing vulnerabilities in public awareness. With over 8,000 investigations launched and 660 charges filed, the report highlighted a sustained whole-of-government effort to strengthen scam prevention, enforcement, and digital literacy across 2025.

Scams Identified

- E-commerce scams (significant year-on-year increase)
- Phishing scams targeting banking and payment credentials
- Investment scams exploiting online platforms and social media
- Self-effected scams where victims voluntarily transfer funds after deception
- Declines observed in fake friend calls, malware-enabled scams, and social media impersonation

Actions for Firms

- Enhance monitoring for patterns linked to e-commerce, phishing, and investment scams
- Strengthen customer education on self-effected scam risks and digital hygiene
- Collaborate more closely with SPF and MAS to support rapid fund-freezing and recovery
- Integrate emerging scam typologies into fraud analytics and behavioural monitoring models
- Review escalation procedures to ensure faster intervention when customer behaviour deviates from typical patterns

Singapore Fraud Key actions

01

Enhance Scam Prevention and Public Awareness

Strengthen organisational preparedness for rising scam typologies by aligning prevention strategies with MAS, SPF, and CSA guidance.

02

Strengthen Customer and TM Controls

Upgrade fraud-detection engines with behavioural and device-intelligence rules, tuned to detect phishing indicators, abnormal wallet provisioning, and account-takeover patterns.

03

Reinforce Controls Around Impersonation and Social Engineering Risks

Expand technical safeguards to protect customers from authority-themed scams and sophisticated social engineering attempts.

5.3 Digital Assets

Singapore continued to advance a measured, risk-focused approach to digital asset regulation in 2025, prioritising strong safeguards against ML, terrorism financing, and cross-border regulatory arbitrage. MAS maintained its longstanding stance that innovation in digital finance must be matched by robust governance, licensing discipline, and stringent conduct standards, particularly for activities with high ML/TF exposure. Throughout the year, the Authority refined its framework to close gaps arising from offshore-facing business models, strengthen oversight of intermediaries, and ensure that virtual asset service providers operating in or from Singapore apply controls consistent with international expectations, including FATF's standards for VASPs.

NEW: MAS Clarifies Licensing Requirements for Digital Token Service Providers (DTSPs)

In June, the MAS issued a significant clarification to the regulatory regime governing Digital Token Service Providers (DTSPs). Effective 30 June 2025, all DTSPs operating from Singapore, including those serving exclusively overseas clients, must obtain a licence under the Financial Services and Markets Act 2022 (FSMA).

MAS emphasised that the licence threshold is intentionally high, signalling that approvals will be granted only in exceptional circumstances. Unlicensed providers that continue servicing foreign customers after the effective date will be required to cease operations. The revised regime reflects MAS's continued focus on mitigating ML/TF risks associated with digital asset flows originating from, or routed through, Singapore.

Licensed entities that already serve customers in Singapore may continue to service overseas clients, provided they remain compliant with existing AML/CTF/CPF obligations and consumer protection requirements under MAS rules. This ensures regulatory continuity while preventing regulatory arbitrage through cross-border business models.

Singapore Digital Assets Key actions

01

Sustain Compliance with DTSP Licensing Obligations

Ensure that ongoing DTSP operations remain fully aligned with FSMA requirements and that post-implementation governance continues to meet supervisory expectations.

02

Strengthen AML/CTF Controls Across All VASP Activities

Apply enhanced CDD, SoF/SoW, sanctions screening, and blockchain analytics across all virtual-asset exposures, capturing high-risk wallets, mixer activity, and cross-border layering behaviour.

03

Prevent Regulatory Arbitrage and Ensure Cross-Border Consistency for VASPs

Apply MAS-aligned controls uniformly to domestic and foreign customers, closing gaps that could enable regulatory arbitrage.

5.4 Conclusion

Taken together, Singapore's recent reforms, enforcement actions, and thematic priorities point to a fundamentally higher baseline for financial crime risk management. The focus is no longer on whether firms have frameworks in place, but on whether those frameworks are fully implemented, evidenced, and resilient under pressure. Boards, senior management, and control functions are expected to translate MAS's expectations on AML/CTF/CPF, fraud, and digital assets into clear accountability, robust documentation, and day-to-day control discipline across all lines of defence.

Looking ahead to 2026 and beyond, MAS signalled that lessons from major enforcement cases, payments-sector sanctions, and scam trends will be hard-wired into future thematic inspections and guidance. Firms that invest in explainable, data-driven controls, cross-border consistency, and a credible culture of deterrence will be best placed to demonstrate that their frameworks are not just compliant on paper, but effective in practice. The direction of travel is clear: FIs operating in Singapore are required to evidence real control effectiveness, transparent governance, and sustained commitment to the integrity of the financial system.

6 Global

In 2025, international standard setters intensified expectations for accountability, transparency, and proportionality in AML/CTF. FATF reforms strengthened beneficial ownership, Travel Rule compliance, and oversight of AI, virtual assets, and online exploitation. Wolfsberg guidance reinforced risk-based monitoring, payment transparency, and technology-enabled controls. Firms must not only comply with these standards but demonstrate operational effectiveness through documented metrics, responsive escalation, and robust model governance. Boards should prioritise cross-border information sharing, adoption of advanced analytics, and continuous oversight to ensure frameworks remain effective and proportionate.

What this means in practice

International standard setters are establishing clear expectations for national frameworks and the approaches of firms operating within them.

In practice, this means that firms can ensure:

- Proportionality to risk informs control operations.
- Travel Rule readiness is in place.
- Ongoing awareness of FC threats emerging from new technologies, reflected in processes.
- Decisions are documented and traceable, with clear governance structures and expectations.
- Understand their customers, from ownership structures to payment behaviours.

6.1 FATF

Having revised core elements of its Standards, the Financial Action Taskforce (FATF) sought to embed proportionality in the global AML/CTF regime and simultaneously incorporate new and evolving threats. Updates to the Recommendations, new guidance on financial inclusion, and reports on TF all point towards a regulatory philosophy that prioritises targeted, risk-based measures. The FATF also sounded a note of caution: significant deficiencies persist across jurisdictions, from weak beneficial ownership transparency and widespread non-compliance with Travel Rule requirements, to uneven application of the risk-based approach and ongoing gaps in TF and payment transparency controls. Without stronger international cooperation to close these weaknesses, criminal actors will continue to exploit inconsistent supervision and fragmented enforcement.

FATF 2025: A Year of Structural Reform, Evolving Threats, and Practical Expectations for Firms

Across its three plenaries in February, June, and October, FATF used 2025 to drive some of the most substantive changes to global AML/CFT standards in recent years. Under the Mexican Presidency, the organisation sharpened its focus on proportionality and effectiveness, tightened oversight of jurisdictions with systemic deficiencies, and expanded its attention to emerging threats linked to online harms, virtual assets, and AI. Together, these developments signal a clear shift towards more agile, outcomes-driven global frameworks and greater expectations on both countries and FIs.

Strengthening Supervision Through Jurisdiction Monitoring

FATF's jurisdiction listings evolved steadily throughout the year, reaffirming expectations for national frameworks, and reminding firms of the importance of continual reassessments of jurisdictional risk.

- **February**: Kenya and Namibia removed from Increased Monitoring, with Monaco and Venezuela added, and the Democratic Republic of the Congo lifted from the Call for Action list.
- **June**: Laos and Nepal were added to the grey list, while the Philippines exited following successful implementation of its action plan.
- **October**: Burkina Faso, Mozambique, Nigeria, and South Africa all removed from Increased Monitoring after sustained reforms. FATF updated its public statement on Iran and reaffirmed the suspension of Russia's membership.

Embedding Proportionate, Risk-Based Standards

2025 saw material reforms to the FATF Standards aimed at making AML/CFT regimes more proportionate and practical to implement.

- **February**: Recommendation 25 revisions strengthened beneficial ownership transparency for legal arrangements, responding to persistent global vulnerabilities.
- **June**: FATF Standards updates introduced proportionality enhancements to Recommendation 1 and interpretive notes for Recommendations 10 and 15, clarifying risk-based approaches for low-risk CDD measures, new technologies, and financial innovation.

Persistent Weaknesses in Virtual Asset Compliance

FATF maintained pressure on jurisdictions to accelerate implementation of AML/CFT measures for virtual assets.

- **February**: Over half of assessed jurisdictions remain non-compliant with the Travel Rule, due to fragmented regulation, inconsistent supervisory models, and technical challenges in data transmission, particularly in decentralised environments and transactions involving self-hosted wallets.
- **June**: FATF endorsed further work on payment transparency and Travel Rule alignment as cross-border Virtual Asset (VA) activity expands.

Expanding the Scope to New and Emerging Threats

FATF assessed and informed states of several emerging threat areas throughout 2025, demonstrating how technology both enables crime and can be used to detect it in the process.

- **February**: FATF reaffirmed its priority focus areas of TF and global asset recovery.
- **June**: Report on financial flows linked to online child sexual exploitation, highlighted the role of financial intelligence in disrupting digital-first harms.
- **October**: 'Horizon Scan' tool launch examined illicit finance risks associated with AI and deepfakes, including their potential use in cyber fraud, identity spoofing, and social engineering schemes.

Improving Global Consistency and Accountability

A notable theme across the year was FATF's drive for more consistent and effective implementation:

- **February and June**: Focus on strengthening beneficial ownership transparency at national levels.
- **October**: Release of new FATF mutual evaluation methodology. Belgium and Malaysia were the first jurisdictions subject to a more disciplined, time-bound follow-up process requiring delivery of key actions within three years.

2025 Plenary Overview

Plenary	Removed	Added	Grey List
February	Philippines	Lao PDR, Nepal	Algeria, Angola, Bulgaria, Burkina Faso, Cameroon, Côte d'Ivoire, Croatia, DR Congo, Haiti, Kenya, Lao PDR, Lebanon, Mali, Monaco, Mozambique, Namibia, Nepal, Nigeria, South Africa, South Sudan, Syria, Tanzania, Venezuela, Vietnam, Yemen
June	Croatia, Mali, Tanzinia	Bolivia, Virgin Islands (UK)	Algeria, Angola, Bolivia, Bulgaria, Burkina Faso, Cameroon, Côte d'Ivoire, DR Congo, Haiti, Kenya, Lao PDR, Lebanon, Monaco, Mozambique, Namibia, Nepal, Nigeria, South Africa, South Sudan, Syria, Venezuela, Vietnam, Virgin Islands (UK), Yemen
October	South Africa, Nigeria, Mozambique, Burkina Faso	None	Algeria, Angola, Bolivia, Bulgaria, Cameroon, Côte d'Ivoire, DR Congo, Haiti, Kenya, Lao PDR, Lebanon, Monaco, Namibia, Nepal, South Sudan, Syria, Venezuela, Vietnam, Virgin Islands (UK), Yemen

UPDATED: FATF Travel Rule (Recommendation 16) Amendments

The FATF approved major updates to Recommendation 16 (the Travel Rule), tightening requirements for cross-border payment transparency. The changes, agreed at the June FATF Plenary in collaboration with The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), are designed to reduce fraud, minimise errors, and strengthen transparency in cross-border payment flows. MONEYVAL was brought into the process because it oversees AML/CTF evaluations across much of Europe, and its involvement ensures that the updated Travel Rule is implemented consistently across both FATF members and the wider group of European jurisdictions under regional supervision.

The revisions bring greater clarity to the allocation of responsibilities across the payment chain, confirming which actors are accountable for ensuring complete and accurate data is maintained within payment messages. They also introduce standardised requirements for information accompanying peer-to-peer cross-border payments above a defined threshold, a move aimed at creating global consistency and improving traceability.

In recognition of the operational risks linked to payment messaging, the FATF mandated the use of tools specifically designed to detect and mitigate fraud and error within the payment process. Furthermore, the amendments clarify the treatment of card transactions, reaffirming their exemption from the full scope of Recommendation 16 but refining the definition of "purchase of goods and services" to provide greater certainty to firms.

By strengthening data integrity requirements and embedding fraud controls within the Travel Rule, the FATF reinforced its expectation that firms adopt a more proactive, technology-enabled approach to safeguarding payment transparency.

Guidance and Reports

UPDATED: FATF Guidance on Financial Inclusion and the Risk-Based Approach

In June, the FATF issued updated guidance on financial inclusion relating to Recommendation 1, reaffirming its commitment to ensuring anti-financial crime frameworks support, rather than hinder, access to the financial system. The guidance underscores the importance of a risk-based approach, encouraging both jurisdictions and private sector firms to design AML/CFT measures that promote access to formal financial services for underserved populations - including low-income communities, rural customers, and undocumented individuals, without reducing vigilance.

In practice, this means FIs may apply simplified CDD where risks are demonstrably minimal. Drawing on international case studies and best practices, the FATF guidance provides regulators and firms with practical tools to strike a balance between mitigating illicit finance and promoting financial inclusion. By embedding proportionality into supervisory and institutional approaches, the FATF aims to reduce the unintended consequences of financial exclusion while maintaining global resilience against financial crime.

NEW: FATF Report on Evolving Terrorist Financing Risks

In July, the FATF published its Comprehensive Update on TF Risks highlighting major gaps in countries' ability to detect and disrupt modern TF threats. The FATF pointed to weak visibility over online financial flows, poor beneficial ownership data, inconsistent application of the risk-based approach, and widespread non-compliance with the Travel Rule, all of which leave blind spots that criminals can exploit. For FIs, this means increased expectations around monitoring online-enabled typologies, verifying ownership structures, and strengthening controls around virtual asset activity. The report found that terrorist actors continue to exploit both traditional and digital channels to move funds, combining cash couriers, hawala networks, shell structures such as NPOs and trusts, and increasingly, digital methods including online platforms, crowdfunding, and virtual assets.

The report also highlights threats presented by decentralised and technology-enabled funding mechanisms, with terrorists using social media and digital payment tools to conceal and distribute resources. 69% of jurisdictions assessments identified serious deficiencies in abilities to investigate, prosecute, or secure convictions for TF, leaving critical vulnerabilities unaddressed. The report calls for stronger public–private collaboration, the development of technical capabilities within FIs, and enhanced oversight of NPOs to prevent their misuse.

NEW: FATF, Egmont Group, INTERPOL and UNODC – Handbook on International Cooperation Against Money Laundering

Four major international bodies, the FATF, Egmont Group, INTERPOL, and the United Nations Office on Drugs and Crime (UNODC), jointly launched a Handbook on International Cooperation against ML. The initiative is intended to strengthen cross-border collaboration among FIUs, law enforcement, and prosecutors, addressing persistent challenges in pursuing illicit assets across jurisdictions. The handbook highlights the value of informal cooperation mechanisms, such as secure communication channels, rapid response frameworks, and joint analyses, in complementing slower formal processes. Real-world case studies highlight how coordinated multi-country operations have led to successful asset seizures and convictions.

To provide practical support, the publication includes three tailored guides: one for FIUs, one for law enforcement agencies, and one for prosecutors. Each outlines tools and approaches for collaboration and cooperation, streamlining intelligence sharing, and accelerating cross-border investigations. Positioned as a key resource ahead of the 2026 UN Crime Congress in the UAE, the

handbook reinforces the global message that recovering illicit proceeds and disrupting ML networks requires timely and coordinated action beyond borders. It represents a renewed commitment by international standard-setters to dismantle the structural barriers that hinder effective financial crime enforcement.

6.2 Wolfsberg Group

The Wolfsberg Group continued to position itself as a leading industry standard-setter in 2025, advancing practical guidance across payments, monitoring, and digital assets. Its publications this year emphasise flexibility, proportionality, and innovation, reinforcing the need for FIs to move beyond procedural compliance. Whether through the refinement of the risk-based approach, the adoption of more effective suspicious activity monitoring, or the application of controls to fiat-backed stablecoin issuers. In practice, the Group is calling for controls that evolve with risk: intelligence-led monitoring rather than static rules, structured model governance for financial crime tools, and deeper due diligence and wallet-level transparency for stablecoin-related activity.

NEW: Wolfsberg Group Statement on the Risk-Based Approach

The Wolfsberg Group released an updated statement on the RBA in July, its first revision since the original publication in 2006. The statement aligns with the FATF definition of the RBA and provides clearer expectations on how FIs should structure financial crime risk management (FCRM) programmes.

The Wolfsberg Group highlights three core elements that must underpin an effective RBA.

1. **Proportionality**: ensuring controls are calibrated to the institution's business model, considering its size, geographic footprint, customer base, and overall risk appetite as defined through robust risk assessments.
2. **Prioritisation**: directing resources and oversight toward higher-risk customers, products, and activities rather than spreading controls uniformly.
3. **Effectiveness**: moving beyond one-size-fits-all compliance programmes and ensuring that FCRMs deliver measurable, forward-looking outcomes capable of adapting to evolving threats.

The updated statement encourages firms to embed flexibility and responsiveness into their FCRMs, ensuring they remain both proportionate and outcome-focused in an increasingly dynamic threat environment.

NEW: Wolfsberg Group – Statement on Effective Monitoring for Suspicious Activity (Part II)

The Group published Part II of its Statement on Effective Monitoring for Suspicious Activity (MSA) in August, titled Transitioning to Innovation. Building on its July 2024 guidance, the paper sets out how FIs can evolve beyond traditional rules-based monitoring and adopt more intelligence-led, dynamic approaches to detecting and reporting financial crime.

The Wolfsberg Group outlines a transition framework based on three key pillars.

1. **Transition and validation:** firms are encouraged to redefine success criteria for their monitoring programmes, prioritising quality outcomes and integrating advanced capabilities such as data analytics and investigator-ready summaries.
2. **Model risk balanced with financial crime risk**: firms are urged to adapt model risk governance to reflect the distinct nature of financial crime detection models, enabling faster adoption of innovative solutions without compromising oversight.
3. **Explainability**: transparency in model design, risk coverage, and use of advanced tools is essential to maintaining trust, regulatory confidence, and effective governance.

The practical resource highlights that effective suspicious activity monitoring must now be forward-looking, outcome-focused, and technologically enabled if it is to keep pace with evolving criminal methodologies and regulatory expectations.

NEW: Wolfsberg Group Guidance on Banking Services to Stablecoin Issuers

In September, the Wolfsberg Group published new guidance on the provision of banking services to fiat-backed stablecoin issuers, marking another step in the Group's efforts to shape industry standards in the rapidly evolving digital asset ecosystem. The paper recognises both the benefits and risks of stablecoins and sets out how FIs can apply a risk-based approach to managing these relationships.

The guidance introduces detailed due diligence expectations, urging firms to develop a deep understanding of the issuer's business model, customer base, including DASPs and corporates, and overall financial crime risk management framework. Tailored expectations for different types of accounts are also detailed, specifically operating accounts, reserve accounts, and settlement accounts.

In addition, the guidance addresses the role of on-chain monitoring, encouraging banks to incorporate blockchain analytics and wallet-level transparency to ensure issuers operate within their stated risk appetite. Proportionality remains a central theme, with oversight measures expected to align with the issuer's risk profile. Ongoing monitoring, through account activity reviews, compliance testing, and escalation procedures for deviations from agreed parameters, is presented as essential to effective governance.

Global Key Actions

01 Embed Proportionate Risk-Based Approaches
Jurisdictions are shifting toward proportionate, outcome-focused AML/CTF expectations. Firms must evidence that controls reflect real risk, in line with FATF's revised Recommendations 1, 10, 15 & 25.

02 Strengthen Payment Transparency and the Travel Rule
FATF's updates to Recommendation 16 require firms to demonstrate end-to-end integrity of payment data across domestic, cross-border, and virtual asset rails. To demonstrate this firms should validate message completeness for all channels (ISO20022, Swift MTs, VA transfers) and produce MU showing missing field rates and remedial actions.

03 Evolve Suspicious Activity Monitoring
Supervisors expect a transition from static rules to intelligence-led, explainable models aligned to FATF and Wolfsberg guidance. Firms should tune, retire or replace legacy systems, incorporating AI-enabled fraud, online harms and crypto-asset typologies into models.

04 Address Digital Assets and Stablecoins
FATF's continued focus on virtual assets requires deeper due diligence, wallet-level transparency, and enhanced monitoring of settlement flows. Firms should conduct structured due diligence questionnaires for stablecoin issues and crypto-asset providers, reviewing reserve attestations, governance and customer types.

05 Enhance International Cooperation
FATF-Egmont-INTERPOL-UNODC guidance underscores the need for faster cross-border intelligence sharing and joint investigations. Firms should update their information sharing procedures to align with FATF's new Handbook e.g. pre-approved templates, expedited approval routes and data-sharing checklists.

06 Counter Emerging TF Risks
FATF's 2025 TF review highlights major weaknesses globally, requiring firms to strengthen online, decentralised, and VA-linked TF detection. In order to address these weaknesses firms could update typologies and triggers to include crowd-funding spikes, crypto-to-cash patterns, deepfake-enabled identity spoofing and NPO misuse. This is not an exhaustive list, firms should do a comprehensive review of potential typologies and triggers before updating models and systems.

6.3 Conclusion

The developments of 2025 reflect a global regulatory environment undergoing rapid and purposeful transformation. Across FATF's structural reforms, enhanced focus on AI-enabled and online harms, tightened expectations for beneficial ownership and payment transparency, and the Wolfsberg Group's practical guidance on monitoring, payments, and stablecoins, international standards are becoming more interconnected, more technologically aware, and more grounded in proportionality than ever before.

FATF's modernised Standards have reshaped the baseline for jurisdictions, strengthening expectations around effectiveness, inclusion, and cross-border cooperation while exposing the evolving nature of TF and decentralised financial crime. In parallel, the Wolfsberg Group has provided firms with concrete pathways to transition towards intelligence-led, risk-based, and innovation-friendly compliance practices that reflect real operational demands rather than procedural formality.

Looking ahead, continued convergence is likely: deeper international cooperation on ML/TF, stricter oversight of digital assets and payment systems, and sustained pressure to close remaining gaps in enforcement and supervision. The challenge for firms will be to balance strengthened controls with accessibility and inclusion, ensuring that as financial crime frameworks strengthen, the financial system remains open, trusted, and resilient.

At firm-level, those which invest in data quality, monitoring innovation, proportionality, jurisdictional risk agility, and robust governance will be best positioned to meet internationally-set standards, and stay ahead of an increasingly complex and technologically enabled threat landscape.

7 Conclusion

As 2026 begins, the international regulatory landscape is undergoing one of its most significant periods of change in over a decade. Global pressures, including the rapid adoption of AI in both criminal activity and supervisory practices, escalating fraud schemes such as the 4,465 fake FCA scam reports filed in early 2025, and large-scale enforcement actions like MAS's issuance of S$27.45 million in penalties across nine institutions, have pushed financial crime risk management to a critical inflection point. Geopolitical volatility, from instability in Ukraine and the Middle East to increasingly complex sanctions frameworks, has further broadened the threat landscape. Europol's 2025 SOCTA underscored how organised crime networks are exploiting these dynamics, blending traditional techniques with digital-first methodologies to evade detection across borders.

Global regulatory frameworks are highlighting the central role of outcome-based, evidence-led supervision, where firms must demonstrate not only that controls exist but that they operate effectively, consistently, and at pace. In many jurisdictions, transparency is a central theme, with identity verification, beneficial ownership reforms, sanctions reporting expansion, and tax-related obligations embedding traceability into the core of the financial system. Sanctions regimes have become more assertive, more complex, and more geopolitical, with circumvention now a supervisory priority in its own right. Fraud, ML cyber-enabled crime, and sanctions evasion are increasingly interconnected, requiring integrated risk frameworks rather than siloed responses.

Technology sits at the centre of this evolution. The mainstreaming of AI, the acceleration of instant payments, and the mainstream regulation of digital assets are reshaping both the risk landscape and the expectations placed on firms. As a result, firms are expected to transform their own data, governance, and model-risk capabilities to keep pace.

Outsourcing and reliance on sector-critical vendors now carry heightened scrutiny, reinforcing that accountability remains with firms regardless of external partnerships.

These shifts demand a fundamental recalibration of operating models. Compliance functions must evolve from static, policy-driven frameworks to dynamic, data-driven, operationally resilient systems capable of detecting sophisticated threats in real time. Firms that continue to treat regulatory reform as a series of incremental adjustments will find themselves increasingly exposed to supervisory challenge, operational strain, and enforcement risk. These developments offer opportunities for a more coherent, harmonised, and intelligence-led approach to financial crime prevention at firm-level.

The organisations best prepared for 2026 and beyond will be those that build and maintain financial crime frameworks that are demonstrably robust, technologically adaptive, and strategically aligned to a regulatory environment defined by complexity, convergence, and speed.

2026 Roadmap

This 2026 roadmap outlines the operational shifts organisations can make to stay ahead of accelerating regulatory expectations, technological disruption, and increasingly complex financial crime risks.

1 Build a Single, Integrated Financial Crime Risk Architecture

Objective: Replace fragmented, typology-based controls with a unified, intelligence-driven ecosystem.

Actions:

- Develop a single enterprise risk taxonomy that aligns AML, sanctions, fraud, cyber, CPF, crypto and payments risk.
- Centralise scenario libraries, red flags, and escalation types to remove duplication and blind spots.
- Embed an enterprise-wide risk assessment framework that maps each risk area to data, controls, systems, and accountable owners.
- Implement cross-functional financial crime committees with clear inputs and outputs.

Outcome: Achieving a unified, intelligence-driven architecture that removes silos and strengthens financial crime risk management.

2 Establish an "Effectiveness by Design" Control Model

Objective: Move from "documented controls" to controls that can prove they work.

Actions:

- Create evidence templates for every material control (tuning records, QA logs, case file rationale, list updates, validation output).
- Embed success metrics and health indicators:
  - detection quality
  - false positives/negatives
  - alert ageing
  - sanctions freezing response times
  - fraud loss reduction
- Introduce quarterly "effectiveness reviews" tied directly to SMF/board attestations.

Outcome: A control environment aligned with the global standard: show me, don't tell me.

3 Build a Resilient, Explainable AI & Model Governance Framework

Objective: Govern AI, analytics, and RegTech with the same rigour as other risk-critical systems and create explainability as a core discipline.

Actions:

- Maintain a unified model inventory and classify models by criticality.
- Implement explainability and validation requirements proportionate to model risk.
- Adopt a "human-in-command" model oversight structure, ensuring decision override, challenge, and documentation.
- Integrate vendor-provided AI tools into internal governance (challenge, drift detection, transparency obligations).

Outcome: AI becomes an auditable, defensible asset, not a regulatory vulnerability.

4 Create a Real-Time Fraud Detection and Response Layer

Objective: Adapt the organisation to instant payments, accelerated fraud, and fast-moving sanctions regimes.

Actions:

- Deploy behavioural analytics, device intelligence, and event-stream monitoring to reduce detection latency.
- Introduce a real-time decisioning "nerve centre" that bridges fraud, AML, sanctions, and cyber response.
- Integrate VoP, geo-intelligence, and identity signals into transaction flows.
- Build operating procedures for high-velocity typologies (APP fraud, sanctions updates, ransomware, mixer use, trade anomalies).

Outcome: The organisation detects and responds at the speed risks now occur.

5 Modernise Data Foundations for Supervisory-Grade Analytics

Objective: Prepare for the era of SupTech-led supervision and cross-border data requests.

Actions:

- Build a financial crime data model spanning customers, transactions, alerts, case outcomes, sanctions hits, wallet activity, and risk indicators.
- Clean and standardise key FC data fields across systems (no critical field should have >1% errors).
- Implement automated lineage mapping so every regulatory request can be answered with traceable data.
- Increase the maturity of MI to move from volume metrics → actionable risk intelligence.

Outcome: Data that is clean, explainable, structured, and able to withstand supervisory deep dives.

6 Strengthen End-to-End Governance and Accountability

Objective: Reinforce the role of senior management in a landscape demanding explainability and proactive oversight.

Actions:

- Define clear accountability for AML, fraud, sanctions, crypto, and operational resilience at SMF/board levels

- Ensure board risk reports include forward-looking analytics, root causes, and thematic trends, not just statistics.
- Implement governance over outsourced and critical third-party providers, including scenario-based oversight and exit strategies.
- Introduce an annual "Financial Crime Assurance Statement" signed by the board.

Outcome: Senior management can evidence that they own, and understand, the risks.

7 Elevate Sanctions Controls into a Strategic Capability

Objective: Enhance sanctions controls by evolving traditional screening into a full-spectrum, intelligence-led risk mitigation capability.

Actions:

- Build a sanctions intelligence team capable of tracking circumvention indicators across maritime, crypto, trade, and corporate structures.
- Implement dynamic risk models for jurisdictions, vessels, counterparties, and digital asset flows.
- Conduct quarterly sanctions threat scenario testing aligned with geopolitical events.
- Integrate sanctions expertise into onboarding, trade finance, payments, and crypto operations.

Outcome: A sanctions framework that can withstand the fastest-moving regulatory risk globally.

8 Integrate Crypto, Digital Assets, and New Payment Rules Into One Control Framework

Objective: Ensure digital assets and instant payments are governed with the same maturity as traditional finance.

Actions:

- Align crypto controls (Travel Rule, wallet assessments, token restrictions, custody governance) with traditional AML frameworks.
- Create unified monitoring combining blockchain analytics with transaction data and sanctions lists.
- Map instant payment exposure, fraud vectors, and sanctions obligations to monitoring rules.
- Prepare governance and staffing structures for stablecoin regimes and MiCA authorisation if relevant.

Outcome: A seamless multi-rule control environment that handles fiat, crypto, and instant payments holistically.

9 Professionalise Cross-Border Intelligence Sharing

Objective: Prepare for an era of international coordination (AMLA, Europol, NECC, FinCEN, OFSI, FATF networks).

Actions:

- Build an FC intelligence hub to collate, structure, and distribute insights internally.
- Develop formal protocols for responding to cross-border authority requests.
- Introduce typology integration cycles: every advisory, sanctions update, NCA/FIU bulletin becomes a control enhancement within a defined time period.
- Partner with industry bodies, utilities, and peer FIs to accelerate intelligence distribution.

Outcome: An organisation that can ingest, operationalise, and act on threat intelligence quickly and consistently.

10 Embed Continuous Adaptation into the Operating Model

Objective: Develop muscle memory for rapid regulatory, technological, and threat evolution.

Actions:

- Run quarterly “threat horizon reviews” covering AI-enabled crime, sanctions escalation, geopolitical shifts, crypto trends, fraud shifts, and vendor/system risks.
- Maintain a regulatory roadmap tracking UK, EU, France, and U.S. developments simultaneously.
- Conduct annual design refreshes of core FC controls.
- Introduce capacity planning to ensure controls scale with growth

Outcome: The organisation becomes structurally capable of keeping pace with regulatory and criminal innovation.

Plenitude RegSight

Plenitude RegSight and its subscription newsletter keep you informed of the evolving regulatory landscape. We conduct weekly horizon scanning to identify new and amended laws, regulations or guidance impacting your organisation's financial crime compliance obligations. As always, we are happy to engage and discuss these developments with you further.

Plenitude has supported several firms, big and small, in implementing financial crime transformation programmes, including robust enhancements of financial crime risk assessment methodologies and risk appetite statements, implementation of financial crime management information and detailed assessments of transaction monitoring capabilities. If you would like to have a chat on what steps might be most appropriate for your firm, drop us an email at enquiries@plenitudeconsulting.com

About this paper:

Authors: Thomas Hudson and Ciarán McMullan
Contributors: Pritika Parkash and Jennifer Sandjo-Mellot
Editors: Imogen Cronin, Olivia Kearney, Orel Garcia, Giles Christou, Leeroy Masamba, Dan Keay and Gary Yeung

Due to length constraints, we have intentionally excluded some events from this paper. However, we have made every effort to include the key developments that have shaped the industry.
This paper serves as a guiding framework and should not be considered legal advice.

8 Appendix: Key 2026 Dates

Date	Jurisdiction	Title	Description
1 January 2026	FR	**UPDATED: Monetary and Financial Code – Tax Evasion and Fraud Provisions**	France's Law No. 2025-127 extends tax transparency obligations to CASPs from 1 January 2026, requiring them to identify account holders' tax residence and, where applicable, controlling persons' tax identification numbers, aligning the sector with broader financial-sector standards to strengthen tax evasion and fraud prevention.
14 January 2026	UK	**UPDATED: The JMLSG launched consultation on changes to Part I guidance**	The JMLSG has opened a consultation, closing 14 January 2026, on updates to Part I guidance clarifying the authority and independence required of MLROs and providing revised data-protection guidance on handling subject access requests linked to SARs, including updated response timelines.
26 January 2026	EU	**NEW: The EBA published a consultation paper on revised Guidelines for the Supervisory Review and Evaluation Process (SREP) and supervisory stress testing**	The EBA launched a consultation, closing 26 January 2026, on updated SREP and stress-testing Guidelines that strengthen supervisory expectations around integrating AML/CTF risks into governance assessments, operational-risk evaluations, stress-testing scenarios, and Pillar 2 capital determinations, while clarifying how financial-crime findings should be documented and communicated.
28 January 2026	UK	**NEW: Moving to a single list for UK sanctions designations**	From 28 January 2026, the UK will consolidate all sanctions designations into a single unified list to simplify screening and reduce operational complexity, with no changes to firms' underlying asset-freeze or reporting obligations.
28 April 2026 (projected)	UK	**NEW: Rules on Account Closure and Notice Periods**	The UK Government will require banks and PSPs to give customers at least 90 days' notice and a clear explanation before closing an account, with legislation, expected to take effect on 28 April 2026, aimed at preventing unjustified "debanking" and enforceable by the FCA.
1 July 2026	EU	**UPDATED: MiCA Implementation and Supervisory Guidance**	Under MiCA's grandfathering period, existing CASPs may continue operating under national regimes until they must obtain a MiCA licence, with several jurisdictions, including Bulgaria, Czechia, Denmark, Estonia, France, Croatia, Italy, Cyprus, Luxembourg, Malta, and Iceland, setting a deadline of 1 July 2026.
Early 2026	UK	**NEW: UK Fraud strategy to be published**	The UK has delayed its Fraud Strategy to early 2026, signalling a push for stronger cross-sector collaboration, greater use of AI in fraud prevention, potential obligations for Big Tech, and heightened expectations on firms as APP scam losses and reimbursements continue to rise.

Date	Jurisdiction	Title	Description
Early 2026	UK	**NEW: Proposed Amendments to the Money Laundering Regulations 2017**	Subject to feedback and Parliamentary scheduling, the final instrument is expected to be laid in early 2026.
2026	UK	**NEW: FCA/PSR Merger**	The FCA and PSR will be merged into a single regulator, the SPSS, with primary legislation to establish the new body scheduled for introduction in early 2026. Legislation to formalise the merger into the new SPSS regulator is expected to be introduced in late 2026.