FINTRAIL

Q4 2025

REGCAP

A summary of the latest FinCrime regulatory news

www.fintrail.com

contact@fintrail.com

Global guidance



Basel AML Index 2025

The Basel Institute on Governance released the 14th annual Public Edition report of the Basel AML Index. The report provides a risk score for jurisdictions based on 17 publicly accessible sources such as FATF, Transparency International and the Global Initiative against Transnational Organized Crime. The 2025 report shows that global money-laundering and financial-crime risks remain largely stagnant, with modest improvements in some high-risk regions (notably parts of Sub-Saharan Africa) counterbalanced by rising risk scores in historically lower-risk areas such as Europe and North America. It also highlights some emerging challenges around effectively applying risk-based approaches and assessing vulnerabilities linked to virtual assets.



The Global Organized Crime Index

The Global Initiative against Transnational Organized Crime released its 2025 Index which shows that organized crime is at a crossroads, with illicit markets reshaping in response to geopolitical, economic and technological changes that enable criminal actors to adapt and expand. Major trends include the rapid growth of non-violent, "invisible" crimes such as financial fraud, cyber-dependent offences and counterfeiting, which are now pervasive and poorly countered by traditional state responses. Some long-standing markets like human exploitation persist, resilience measures (including international cooperation and judicial capacity) have stagnated or weakened, suggesting that state responses are struggling to keep pace with evolving threats.



FATF Asset Recovery Guidance and Best Practices

The FATF's new Asset Recovery Guidance and Best Practices provides a comprehensive, operational roadmap for jurisdictions to strengthen the full lifecycle of asset recovery, from identification and tracing through to freezing, seizure, confiscation and return of criminal assets. It stresses that asset recovery should be a policy and operational priority, with coordinated financial investigations integrated from the outset of serious crime cases and clear inter-agency cooperation domestically and internationally. The guidance encourages broader use of tools such as non-conviction-based confiscation and unexplained wealth measures, enhanced provisional measures to prevent dissipation of assets, and effective management and use of recovered assets, including victim restitution.



IMF AI Projects in Financial Supervisory Authorities - A toolkit for successful implementation

The IMF paper highlights the growing need for financial supervisory authorities to adopt Artificial Intelligence tools to keep pace with the digitalisation of financial services and enhance supervisory effectiveness, including in areas like risk monitoring and data analysis. It proposes a tailored project management methodology for AI implementation that aligns AI initiatives with strategic objectives and addresses the unique risks posed by financial supervision, such as explainability, bias and governance. The report emphasizes that successful AI deployment requires strong governance structures, multidisciplinary teams, robust data practices and sufficient resources, and they recommend iterative, risk-aware approaches to project planning, development and post-deployment monitoring.



FATF Horizon Scan: AI and Deepfakes

The FATF Horizon Scan on AI and Deepfakes examines how artificial intelligence, particularly deepfake technology, is emerging as a significant risk to global AML and CTF frameworks. The report explains that criminals can use AI-generated audio, video, and synthetic identities to commit fraud, impersonate individuals, bypass customer due diligence, and manipulate financial institutions. While acknowledging the legitimate and beneficial uses of AI, FATF emphasizes its dual-use nature and the growing sophistication and accessibility of these tools. The report highlights the need for regulators, financial institutions, and law enforcement to strengthen safeguards, adapt risk assessments, and combine technological solutions with human oversight to stay ahead of AI-enabled financial crime.

UK

HMT AML/CTF Supervision Report

The AML/CTF Supervision Report 2024–25 is HM Treasury's 13th annual supervisory report. It fulfils the obligation under Regulation 51 of the Money Laundering Regulations (MLRs) to publish supervisory data submitted by AML/CTF supervisors. It consolidates data from Public Sector supervisors (FCA, HMRC, Gambling Commission) and Professional Body Supervisors (PBSs), and highlights trends, enforcement outcomes, and supervisory actions across the UK regime. Key highlights from the report include:

- the decision to make the Financial Conduct Authority (FCA) the sole AML/CTF supervisor for the professional services sector (legal, accountancy, trust and company service providers),
- across the AML/CTF supervisory landscape enforcement actions and fines continue to rise, reflecting a more assertive supervisory stance. Some key stats include: 1,085 fines issued, £59.5 million worth of fines issued, 1,939 formal actions taken
- the expansion of dedicated AML/CTF supervision capability (including for cryptoasset firms), and spending more time and budget on supervisory engagement



UK Anti-Corruption Strategy 2025

The UK Anti-Corruption Strategy 2025 sets out a comprehensive, five-year plan to reduce the harm corruption causes to the UK's economy, security and democratic systems. It is structured around three main



pillars: combatting corrupt actors and their funds at home and abroad, tackling corruption vulnerabilities within UK institutions and systems, and deepening international cooperation and resilience against corruption. Key measures include expanding the City of London Police's Domestic Corruption Unit and national law enforcement coordination, strengthening sanctions and prosecution of corrupt actors and professional enablers, improving transparency of beneficial ownership, and piloting new technologies to support complex investigations. The strategy also proposes reforms to the AML/CTF supervisory system by consolidating supervisory functions under the FCA to tighten oversight of professional services. Additionally, it aims to bolster public sector integrity through a new Ethics and Integrity Commission, enhanced vetting in high-risk sectors, and greater transparency around political donations

FCA launches Firm Checker to fight financial crime

The FCA has just launched a new Firm Checker to prevent consumers being scammed by unregulated firms offering fraudulent investment opportunities or scams related to pensions. The lookup will allow people to check whether a firm is authorised and what permissions they have more easily.

Guidance on people with significant control (PSC) requirements

There has been updates to the People with Significant Control (PSC) guidance in the UK including:

- Mandatory identity verification for PSCs has been introduced, requiring all new PSCs (and existing ones within a transition period) to verify their identity with Companies House when appointed or updated. This change aims to enhance transparency and combat fraud.
- The requirement for companies to maintain their own local PSC registers has been removed; instead, all PSC information must be filed and maintained centrally by Companies House.
- New and updated guidance materials clarify how PSC requirements apply to different entity types, including companies, UK Societas, LLPs and eligible Scottish partnerships, and provide practical steps for reporting, updating and verifying PSC data.
- Additional technical guidance reflects changes to statutory forms and reporting processes, including updated Companies House forms that align with the new central reporting and identity verification regime.

These revisions are part of the implementation of wider economic crime reforms and are intended to strengthen ownership transparency, reduce fraud risks, and ensure PSC data remains accurate and verified.



UK FIU SAR Best Practice Guidance

The NCA released updates to its SAR guidance consisting of three core chapters on: (1) Using the SAR Portal, (2) Submitting a SAR, and (3) Understanding Defence Against Money Laundering (DAML) and Defence Against Terrorist Financing (DATF) requests, offering practical, step-by-step advice for reporters across regulated sectors. The guidance clarifies common pitfalls in SAR submissions, emphasises the importance of keeping contact details on the SAR Portal current, and explains the scope and correct use of DAML/DATF requests, including the conditions under which defences can be granted and common misuses to avoid. Regulated entities are expected to review and update internal AML policies and procedures to align with the new best practice principles.



JMLSG Consultation: Part 1

JMLSG launched a consultation on proposed amendments to Part I of its UK AML/CTF Guidance. The consultation focuses on revisions to Chapter 3 and Chapter 6, specifically updating guidance on the role and responsibilities of the MLRO, including monitoring the effectiveness of AML controls, and guidance related to the intersection between data protection and SARs including subject access requests (SAR/DSAR) in the context of suspicious activity reporting. The consultation runs until 14 January 2026.

FCA's findings on risk assessment processes and controls in firm

The FCA conducted a multi-firm review of business-wide risk assessments (BWRA) and customer risk assessments (CRA) as part of its financial crime supervisory work. The FCA found that while most firms have financial crime risk assessments in place, many are insufficiently tailored to their specific business models and fail to clearly identify or evidence key risks. Risk assessment outputs are often poorly integrated into governance, decision-making and control frameworks, with limited documentation of actions taken to mitigate identified risks. Stronger firms demonstrated regular review, senior management oversight and clear linkage between risk appetite, controls and monitoring. Overall, the FCA expects firms to adopt more dynamic, evidence-based and business-specific risk assessment processes to ensure effective financial crime risk management.



UK Government new crypto rules to unlock growth and protect customers

The UK Government has unveiled plans for new, firm and proportionate cryptoassets regulation designed to position the UK as a global hub for digital assets while strengthening protections for consumers and investors. Under the proposals, crypto firms will be brought fully into the regulatory perimeter and regulated by the FCA in a manner similar to other financial products, with requirements on transparency and oversight that aim to boost confidence and deter bad actors. The legislation is expected to come into force from 2027, providing legal clarity and supporting innovation, competition and market growth in the crypto sector. The regime is intended to balance responsible innovation with robust consumer safeguards and help shape global standards for crypto regulation.

The FCA has published various consultations on these rules including:

1. CP25/40 - Rules that will apply to regulated cryptoasset firms
2. CP25/41 - Market abuse regime for cryptoassets
3. CP25/42 - Prudential regime for cryptoasset firms

All consultations are open until 12 February 2026.

UK Government AML/CTF supervision reform: duties, powers and accountability consultation

After providing confirmation that the FCA would now also supervise lawyers, trust or company service providers and accountants, HMT published a consultation on how the reform might look. The proposal includes:

- Registration & gatekeeping: FCA would register all in-scope firms and have powers to approve, refuse, suspend, or cancel registrations.
- Perimeter supervision: The FCA would also actively police the AML/CTF perimeter by identifying unregistered activity and maintaining a public register of supervised firms to improve transparency and deter illicit activity.
- Risk-based supervision: Apply consistent risk-based oversight, including up-to-date risk profiles, targeted desk/onsite reviews, and enhanced information-gathering powers.
- Supervisory tools: Ability to issue directions and require firms to appoint skilled persons to review controls.
- Guidance & intelligence: Provide AML/CTF risk guidance, share intelligence with authorities, support whistleblowing, and improve SAR-sharing with the NCA.
- Enforcement powers: Impose civil penalties, suspensions, prohibitions, public censures, and initiate criminal proceedings, with decisions appealable to the courts.
- Funding & accountability: Supervision funded on a cost-recovery basis, with FCA operationally independent and accountable to HM Treasury and Parliament, while legislative safeguards minimise burdens on firms.

Open Banking: Financial Crime in Open Banking – 2025 Update

The report shows that fraud in open banking payments remains much lower than the wider payments industry, with open banking fraud accounting for just 0.013% of transactions by volume in H1 2025 compared to 0.045% industry-wide, and a similar pattern by value. Although overall fraud volume and value in open banking have decreased year-on-year, there has been a recent slight uptick in fraud that mirrors broader market trends. Authorised Push Payment (APP) scams are the main challenge, making up around 74% of open banking fraud cases, often with higher than average transaction values. The report highlights the importance of adaptive strategies, industry data sharing and transaction risk monitoring tools to strengthen fraud controls across the ecosystem. It also notes emerging threats, including AI-enabled scams, SIM-swap attacks and social engineering, that require ongoing vigilance and collaboration.

FCA financial crime controls in corporate finance firms survey findings

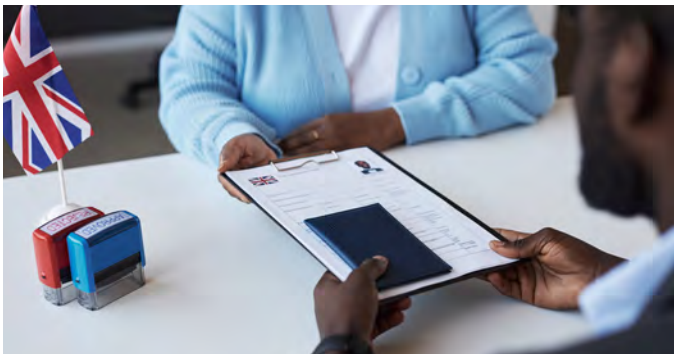
The FCA's survey of over 300 corporate finance firms found that around two-thirds may not fully meet Money Laundering Regulation requirements, with frequent weaknesses in key financial crime controls. Some firms lacked a documented business-wide risk assessment and did not retain documented customer due diligence, despite these being regulatory obligations. On the positive side, most firms reported regular senior management reporting and some maintained risk registers and meaningful management information. The FCA will use these insights to guide supervisory engagement and expects firms to address identified gaps promptly.

Independent review of the Payment and Electronic Money Institution Insolvency Regulations 2021

The independent review of the PEMI Insolvency Regulations 2021 found the framework generally works but identified practical and legal challenges affecting timely access to customer funds. It recommends technical clarifications, clearer definitions, and improved guidance for regulators, insolvency practitioners, firms, and consumers to strengthen confidence and ensure the protection of client money during payment and e-money firm insolvencies.

Regulatory Initiatives Grid - 9th Edition

The Regulatory Initiatives Grid is a bi-annual publication that sets out the pipeline of planned regulatory initiatives across UK financial services over the next 24 months, helping firms and stakeholders anticipate and plan for upcoming policy and rule changes. It is published by the Financial Services Regulatory Initiatives Forum, bringing together key UK regulators and government departments to improve transparency, coordination and predictability of regulatory activity. The December 2025 edition covers multiple live initiatives, including measures to support financial stability, streamline regulation, facilitate innovation (e.g., stablecoins, payments reform) and boost consumer confidence, with around a third being joint initiatives involving multiple authorities. By providing timelines, responsible bodies and likely operational impacts, the Grid supports firms in allocating resources effectively and navigating regulatory change.



UK Government announces new measures to confiscate criminal proceeds from fake immigration lawyers

The UK Government has announced new measures to confiscate the criminal proceeds of individuals illegally posing as immigration lawyers and advisers, using extended powers under the Proceeds of Crime Act granted to the Immigration Advice Authority (IAA). These powers will enable the IAA to trace, freeze and recover illicit gains from illegitimate advisers without relying on police support, with recovered funds reinvested into frontline policing and border security efforts. The move targets rogue operators who have exploited vulnerable migrants for high fees, with some having made millions from fraudulent services. The reforms follow a public consultation and aim to strengthen enforcement against immigration-related fraud while disrupting the financial incentives of such criminal conduct.

OFSI Annual Review 2024 to 2025

OFSI reported significant progress in strengthening the UK's financial sanctions regime in 2024–25, focusing on enhanced compliance support, improved capability and robust enforcement to ensure sanctions are effective and predictable for industry. OFSI expanded its outreach and guidance, including FAQs, targeted advisories and webinars, to help firms understand and implement sanctions. It also deepened international cooperation, including a first Memorandum of Understanding with the US Treasury, and strengthened intelligence capabilities to better detect and disrupt sanctions evasion. Enforcement activity increased with 57 actions taken, including civil penalties and a notable fine against Herbert Smith Freehills for Russia sanctions breaches, reflecting a more intelligence-led, proactive approach to potential violations. Overall, OFSI reported £37 billion of assets frozen under UK sanctions.

Single list for UK sanctions delegations

The UK Government is consolidating its sanctions regime so that the UK Sanctions List (UKSL) becomes the sole authoritative list of all UK sanctions designations from 09:00 GMT on 28 January 2026, replacing the current dual-list system of the UKSL and the OFSI Consolidated List of Asset Freeze Targets. This change aims to simplify compliance, reduce duplication and improve clarity for businesses and industry that screen for sanctions. Organisations must ensure their screening systems, controls and data feeds transition from the OFSI Consolidated List to the UKSL by that date. The guidance also outlines how to prepare internal systems, engage with third-party data providers, and adjust compliance policies ahead of the switch to avoid disruption. Overall, the move is intended to streamline sanctions checks and make the UK sanctions framework more efficient and user-friendly.

SFO's guidance on evaluating a corporate compliance programme

The SFO guidance sets out when and how it will assess a company's compliance programme to inform key enforcement decisions, including whether to prosecute, offer a Deferred Prosecution Agreement (DPA), include compliance terms or a monitor, and consider defences under the Bribery Act 2010 and Economic Crime and Corporate Transparency Act 2023. It explains that the SFO will evaluate the effectiveness and proactive nature of compliance arrangements both at the time of the offence and at the time of reporting or charge, and that strong, genuinely effective programmes can be factors against prosecution or in favour of a DPA. In assessing compliance, the SFO will look beyond policies on paper to how procedures operate in practice, drawing on internal evidence and cooperation from the organisation, with a holistic evaluation of culture, controls and outcomes.

PSR APP Scams reimbursement dashboard for Q2 2025 update

The PSR's APP Scams Reimbursement Dashboard shows early outcomes from the mandatory reimbursement policy for Authorised Push Payment (APP) scams that came into effect on 7 October 2024. In the first nine months of data (to 30 June 2025):

- around £112 million (or 88 % of reimbursable losses) was returned to victims,
- 84 % of claims were closed within five business days, indicating generally timely responses from payment firms,
- approximately 181,000 claims were reported, with 126,000 in scope for reimbursement under the policy, and only a small proportion of claims were rejected because consumers failed to meet the standard of care.

Guidance on the information sharing measures in the Economic Crime and Corporate Transparency Act 2023

The UK Government guidance explains how the Economic Crime and Corporate Transparency Act 2023 allows AML-regulated firms to share information with each other to help prevent and detect economic crime, with protections against breaching confidentiality when conditions are met. Information can be shared directly or via third-party intermediaries, on a voluntary basis, provided UK GDPR requirements are satisfied. The measures are intended to give firms greater confidence to collaborate while maintaining secure handling, audit trails and existing obligations such as SAR reporting.





Europe

EBA PSD2 Peer Review Follow-up Report 2025

The EBA's 2025 follow-up Peer Review on the authorisation of payment institutions and electronic money institutions under PSD2 assesses how Member State supervisors have implemented 2023 recommendations, including those related to AML/CFT frameworks and controls. It finds that although many regulators have improved their supervisory processes, significant divergences remain in how AML/CTF requirements and internal control mechanisms are applied across jurisdictions, which can lead to an uneven regulatory landscape. Supervisors have made progress in assessing applicants' compliance with AML/CTF expectations during the authorisation process, but differences in interpretation and implementation continue to hinder convergence in supervisory outcomes. The review highlights that incomplete or poor-quality applications, including deficiencies in AML/CTF documentation and controls, are a key driver of longer authorisation timelines.

EBA report identifies opportunities for SupTech tools in supervision and enforcement

The EBA analysed how the EU Artificial Intelligence Act (AI Act) intersects with existing EU banking and payments legislation to clarify regulatory and supervisory implications for the financial sector. It found no major contradictions between the AI Act and sectoral financial services laws (e.g., CRR/CRD, PSD, DORA) and concluded that the AI Act is largely complementary, though firms may need to integrate the requirements of both frameworks in practice. The report underscores that multiple authorities, such as prudential/conduct supervisors and market surveillance bodies, will be involved in overseeing compliance, highlighting the need for strong cooperation across supervisors to implement the AI Act effectively. Looking ahead, specific EBA actions in 2026–27 will focus on fostering supervisory alignment and providing input into EU guidance on the interface between the AI Act and financial sector law.

The European Supervisory Authorities designate critical ICT Third-party providers under DORA

The EBA and European Securities and Markets Authority (ESMA) have published the first list of designated critical ICT third-party providers under the Digital Operational Resilience Act (DORA) as part of implementing its oversight framework. The providers on the list support critical or important ICT services, such as core infrastructure, data and business services, for financial institutions across the EU, reflecting their systemic importance and limited substitutability. Amazon, Google, Microsoft, Bloomberg and LSEG are a few to note.

EBA responds to the European Commission Anti-Money Laundering Authority (AMLA) Mandates

The EBA has formally responded to the European Commission's Call for Advice by setting out key risk-based and proportionate regulatory building blocks for the forthcoming EU AML/CFT framework that will underpin the Authority for Anti-Money Laundering (AMLA). The advice covers draft regulatory technical standards (RTS) on risk assessment methodologies for obliged entities and supervisors, criteria for AMLA's direct supervision scope, enhanced customer due diligence requirements, and a structured approach to classifying breaches and setting sanctions under the new regime. The EBA will transfer its AML/CFT mandate to AMLA by 31 December 2025 but will continue to contribute from a prudential perspective and cooperate closely with the new authority.

European Central Bank Digital Euro Project

The European Central Bank (ECB) announced that it has successfully completed the preparation phase of its digital euro project and is moving into the next phase to ensure technical readiness for potential issuance. If the necessary EU legislation is adopted during 2026, the ECB could begin a pilot exercise by mid-2027 and aims to be ready for a possible first issuance of a digital euro by 2029. The initiative is intended to modernise the euro's role in payments, support innovation and preserve privacy and monetary sovereignty as digital transactions grow. Final decisions on issuance and timing will depend on the adoption of the legislative framework.

EU to diverge from FATF and blacklist Russia

The European Commission has officially added Russia to the EU's list of "high-risk third countries" due to strategic deficiencies in its AML/CFT framework. This designation means that financial institutions and other obliged entities across the EU must apply enhanced due diligence and heightened vigilance when dealing with transactions involving Russia or Russian counterparties.

EBA Report on Tackling ML/TF Risks in Crypto-Asset Services through Supervision

The EBA's October 2025 report highlights ML/TF risks in crypto-asset services and provides guidance for EU supervisors under MiCA and the revised AML/CFT framework. Key issues include unauthorised operations, weak governance, opaque ownership, and attempts to exploit regulatory gaps. The report stresses the need for robust authorisation, beneficial ownership transparency, strong AML controls, and cross-border supervisory cooperation. It aims to help competent authorities implement the new regulatory framework effectively and ensure consistent, risk-aware supervision of crypto-asset activities.

EBA Report on Tackling ML/TF Risks in Crypto-Asset Services through Supervision

The EBA has published a report showing that competent authorities across the EU/EEA have made significant progress in strengthening AML/CTF supervision of banks following multi-year implementation reviews. Most supervisory authorities now apply risk-based strategies, have dedicated AML/CFT plans and manuals, and are using supervisory tools more strategically to ensure consistency and effectiveness. There has also been improved cooperation and information exchange with domestic public authorities and across borders, although some jurisdictions still need to enhance cooperation with prudential supervisors. The report will inform the new body Authority for Anti-Money Laundering (AMLA) and supports its future indirect supervisory role, while work continues to address outstanding recommendations.

EBA strengthens cross border supervisory cooperation with third countries

The EBA has updated its Guidelines on the equivalence of confidentiality and professional secrecy regimes for third-country authorities to support stronger cross-border supervisory cooperation. The revised framework expands on the 2022 Guidelines to reflect new requirements under the Markets in Crypto-Assets Regulation (MiCAR) and the latest equivalence assessments. Under the updated Guidelines, the confidentiality regimes of several non-EU authorities, including those in Australia, China, Montenegro, Peru, Serbia and the UK, are now recognised as equivalent to EU standards, facilitating secure exchange of supervisory information. The changes also streamline definitions and clarify how competent authorities should apply the equivalence framework when sharing information and cooperating internationally. These measures aim to enhance supervisory convergence and effective cooperation between EU and third-country regulators.

AMLA draft regulatory technical standards on the assessment of the inherent and residual risk profile of obliged entities

The report provides a harmonised, risk-based framework for EU supervisors to assess ML/TF risks in financial sector obliged entities. It sets common data points and indicators for evaluating inherent risk, control effectiveness, and residual risk, guiding supervision and inspection frequency. The methodology ensures consistent, comparable risk assessments across Member States, with reviews proportionate to entity size and risk. Once adopted, it will support more effective and uniform AML/CFT supervision across the EU.



Key typologies and warnings

NCA Amber Alert: "Networks and Shadow Fleets"

The NCA, through the National Economic Crime Centre (NECC) in partnership with OFSI and the FCDO, issued an Amber Alert (0788-NECC) in November 2025 warning financial institutions, maritime operators and compliance teams about sophisticated sanctions-evasion networks and "shadow fleets" used by sanctioned states such as Russia, Iran and North Korea to maintain revenue flows from commodity exports, particularly oil and gas. These shadow fleets consist of hundreds of ageing vessels with opaque ownership structures that are regularly renamed, reflagged under permissive registries and insured through shell entities to disguise their true purpose and avoid enforcement. The alert highlights risk indicators and typologies that should be integrated into sanctions risk assessments and compliance frameworks, and urges firms to enhance due diligence, monitoring and reporting of suspicious activity to both the NCA's SAR Portal and OFSI. This alert builds on an earlier Red Alert on the "Shadow Fleet Sanctions Evasion and Avoidance Network" and underscores the importance of cross-sector vigilance against evolving sanctions evasion typologies.



HMRC Trade-Based Money Laundering (TBML) handbook

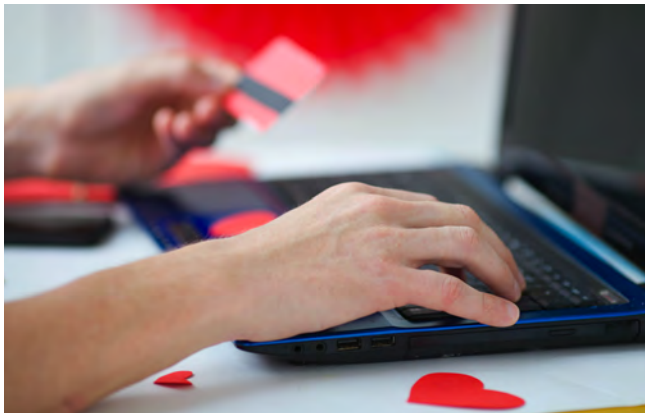
HMRCs published its TBML handbook in October 2025. It provides practical guidance on identifying and addressing trade-based money laundering, a method where criminals disguise illicit proceeds through distorted international trade transactions such as falsified invoices, incorrect pricing, or phantom shipments. It explains common TBML techniques (e.g., over/under-invoicing, multiple invoicing, misdescription) and how trade and customs data can be used to spot red flags.

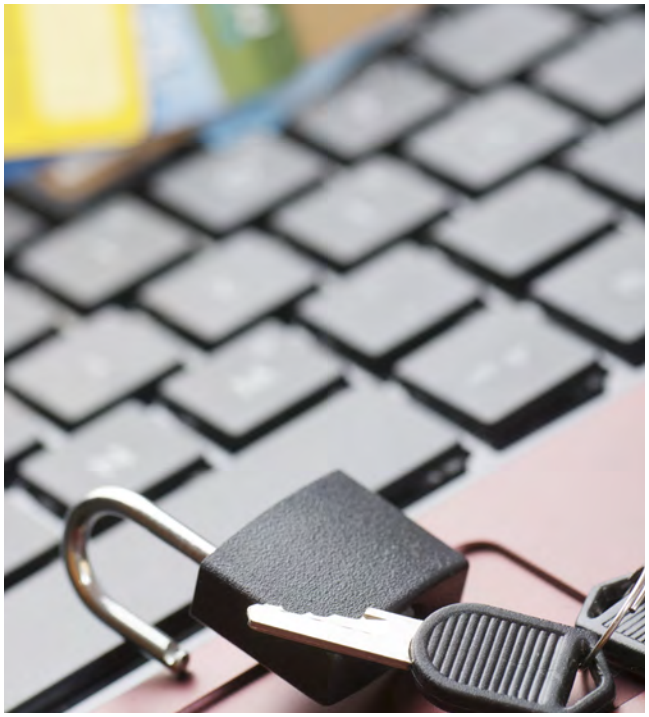
FinCEN identifies $9 billion of Iranian shadow banking activity in 2024

FinCEN's Financial Trend Analysis found roughly $9 billion of possible Iranian shadow banking flows in 2024 moving through U.S. correspondent accounts, revealing how Iran's sanctions-evasion networks operate across global financial systems. A major typology involves the use of foreign shell companies, often with no verifiable business activity, to send and receive large sums, with around $5 billion linked to these entities transacting via non-resident accounts tied to Hong Kong and the UAE. Oil and petrochemical front companies are another key typology, engaging in roughly $4 billion of transactions that potentially mask illicit oil sales and proceeds. Other observed methods include shipping/logistics intermediaries facilitating transport of sanctioned commodities, investment firms providing access to international markets, and technology procurement entities moving funds that may support Iran's weapons and military acquisition programs. The analysis also highlighted correspondent banking exploitation, including through U.S., UK and Singapore branches, showing how sanctioned networks use legitimate banking corridors to move illicit funds across jurisdictions.

FCA's multi-firm review on combating romance fraud

The FCAs multi-firm review found that romance fraud is increasing in scale and complexity, with reported losses exceeding £106 million and many victims reluctant to disclose the true purpose of payments, making detection hard. A high proportion of scams originated on online platforms, and fraudsters often start with low-value requests that appear normal, limiting firms' ability to identify suspicious patterns. Some firms demonstrated good practice in detection and support, using data signals to flag unusual transactions and providing compassionate, tailored engagement with victims. However, many firms missed red flags, failed to challenge implausible explanations, and did not consistently analyse payments beyond Faster Payments, reducing the effectiveness of controls.





FINTRAC: Operational Alert — Laundering the proceeds of online child sexual exploitation report

The report is an operational alert from Canada's FINTRAC designed to help reporting entities identify financial transactions that may be linked to the laundering of funds from online child sexual exploitation. It was developed with multiple domestic and international law-enforcement and financial partners as part of Project Shadow, a public-private initiative to improve detection and prevention of such crimes. The alert outlines emerging money-laundering indicators based on FINTRAC's analysis of suspicious transaction reports and other data, such as frequent low-value transfers, travel-related expenditures, and payments via peer-to-peer platforms or adult entertainment services.



Stories from around the world

MAS Guidelines for AI Risk Management

The MAS AI Risk Management Guidelines set out proposed supervisory expectations for how financial institutions in Singapore should govern, oversee and manage risks arising from the use of AI technologies, including generative AI and autonomous systems, across their operations. Key expectations include:

- Board and senior management oversight of AI risk, embedding AI risk considerations into enterprise-wide governance and risk culture.
- Robust AI risk management frameworks with clear policies, procedures and systems that identify, assess and govern AI use throughout its lifecycle.
- Lifecycle controls on AI systems, including risk materiality assessments, data governance, fairness, transparency, explainability, human oversight and third-party risk management.
- Expectations that institutions maintain inventories of AI systems and undertake regular reviews of risks as AI tools evolve.

The consultation on these guidelines is open through **31 January 2026.**

Canada's Anti-Fraud Strategy and new Financial Crimes Agency

In October 2025, Canada's Minister of Finance announced the government's first national anti-fraud strategy to tackle rising financial scams, economic abuse, and related crimes, especially affecting seniors and other vulnerable groups. The strategy will introduce legislative changes requiring banks to implement stronger fraud prevention policies and give consumers more control over risky account features. A new Financial Crimes Agency will be created by spring 2026 to lead investigations into complex financial crimes such as online scams, money laundering, and organized criminal activity, and to help recover illicit proceeds. The government also plans to work across sectors, including technology and telecommunications, to strengthen fraud detection and response.





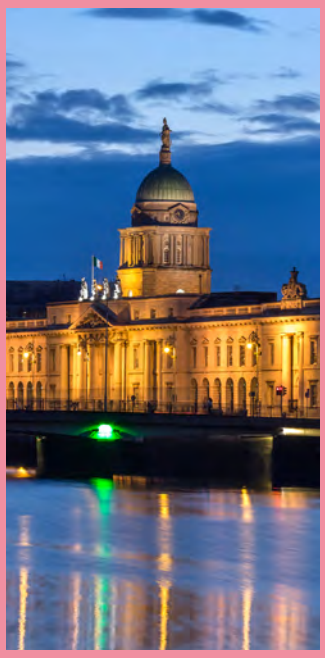
UAE Federal Decree-Law No. 10 of 2025 on Combating ML/TF/PF

The UAE has enacted Federal Decree-Law No. 10 of 2025 on Combating Money Laundering, Terrorist Financing, and Proliferation Financing, fully aligning the national framework with the latest FATF standards. The law operationalises findings from the National Risk Assessment (NRA) and the 2024–2027 AML/CFT/CPF Strategy, introducing practical measures to strengthen financial integrity. Key reforms are organised around eight pillars:

- **National Coordination:** Enhances the role of the renamed National Anti-Money Laundering and Combatting the Financing of Terrorism and Proliferation Financing Committee (NAMLCFTPFC) for cross-agency coordination.
- **Virtual Assets:** Implements registration, licensing, and supervision requirements for virtual asset service providers (VASPs).
- **Legal Persons and Arrangements:** Improves transparency and beneficial ownership information access.
- **Non-Profit Organizations:** Protects against misuse while supporting legitimate charitable activity.
- **Proliferation Financing:** Enforces strict controls aligned with UN Security Council resolutions.
- **Asset Recovery and Management:** Expands freezing, confiscation, and recovery powers, establishing a dedicated Asset Recovery Management Entity and empowering the FIU to issue immediate freezing orders.
- **Sanctions and Enforcement:** Introduces proportionate administrative and criminal penalties to ensure deterrence.
- **Enhanced FIU Powers:** Strengthens the FIU's authority to analyze suspicious transactions, exchange information internationally, and detect illicit financial flows early.

CBI Financial Crime Bulletin - First Edition

The Central Bank of Ireland released its first Fin Crime Bulletin, with key insights on AML.CFT risk assessments, crypto and payments, fraud and scams and sanctions screening systems testing. The Bulletin explains CBI's integrated supervisory approach and rollout of enhanced, sector-specific risk evaluation questionnaires to better inform risk-based supervision. The update notes ongoing MiCAR authorisations for crypto asset service providers, EU requirements like the Recast Funds Transfer Regulation and Travel Rule, and increased supervisory focus on robust AML/CFT systems following a major enforcement action against Coinbase Europe Limited. The Bank also warns that fraud and scams are growing with digitalisation and outlines its work with authorities (including Trusted Flagger status) to bolster prevention and awareness. Finally, it covers financial sanctions obligations, including screening challenges and compliance with evolving EU restrictive measures, and provides an overview of AMLA's progress and upcoming EU AML Package deliverables



Enforcement actions

UK: Nationwide Building Society

The FCA fined Nationwide Building Society £44,078,500 in December 2025 for inadequate anti-financial crime systems and controls between October 2016 and July 2021. Nationwide failed to maintain effective due diligence, risk assessments and transaction monitoring for its personal current account customers, even as it knew some were using accounts for business activity without the right controls in place. As a result, the firm missed multiple red flags, including a case where a customer received £27.3 million in fraudulent Covid furlough payments, of which around £800,000 remains unrecovered by authorities. Although Nationwide has since undertaken a large-scale transformation of its financial crime framework and cooperated with the FCA, the prolonged control weaknesses exposed significant ML/TF risks. The fine was reduced from nearly £63 million thanks to early resolution discount provisions.

Lesson: Key learnings include ensuring robust transaction monitoring is in place which monitors for atypical account usage (e.g. personal accounts being used commercially) and timely remediation matters (i.e. known control weaknesses should be assessed quickly).



Ireland: Coinbase Europe

The CBI fined Coinbase Europe Limited €21,464,734 on 6 November 2025 for serious AML and CTF monitoring failures under the Criminal Justice (Money Laundering and Terrorist Financing) Act 2010. Between April 2021 and March 2025, faults in Coinbase's transaction monitoring system meant over 30 million transactions worth more than €176 billion were not properly monitored for suspicious activity, representing about 31 % of the firm's transaction volume during the affected period. It took the firm almost three years to complete retrospective monitoring, leading to 2,708 Suspicious Transaction Reports (STRs) being submitted for activity linked to suspected money laundering, fraud, drug trafficking, cyber-attacks and child sexual exploitation. The fine was originally set at nearly €30.7 million but reduced by 30 % under the Central Bank's settlement scheme for early resolution.

Lesson: Key lessons include (1) effective real-time monitoring is essential to detect and report suspicious activity; system configuration errors can expose firms to significant AML/CTF risk and penalties, (2) delayed remediation and reporting dramatically weaken the effectiveness of compliance regimes and can undermine law enforcement efforts.



US: Paxful Holdings

FinCEN assessed a $3.5 million civil penalty against Paxful, Inc. and Paxful USA, Inc. for willful violations of the Bank Secrecy Act (BSA), including failing to register as a money services business, implementing an effective AML program, and filing suspicious activity reports (SARs). The peer-to-peer crypto trading platform facilitated over $500 million in suspicious activity involving illicit actors and high-risk jurisdictions such as Iran, North Korea and Venezuela. FinCEN cited systemic disregard for AML obligations, noting the company's inadequate compliance infrastructure over an extended period, though it acknowledged mitigating factors including leadership changes and remediation efforts.

Lesson: Virtual asset service providers must implement robust, risk-based AML programs, properly register as money services businesses, and report suspicious activity promptly. Firms cannot rely on weak or manual controls for high-risk transactions, especially involving high-risk jurisdictions or illicit proceeds, as failure to do so can result in substantial civil and criminal penalties.



UK: Institute of Certified Bookkeepers

The FCA issued a public censure to the Institute of Certified Bookkeepers in December 2025 (the FCA's first enforcement action against a professional body supervisor) for serious deficiencies in its AML supervision of over 3,000 bookkeepers. ICB failed to adopt an adequate risk-based approach and did not effectively monitor members' compliance with the Money Laundering Regulations 2017, most notably suspending all onsite and virtual inspections for nine months, which significantly weakened oversight and increased sector AML risks. Key findings were:

- During the Relevant Period, 1 January 2022 to 26 July 2023:
  - » Did not effectively monitor its members
  - » Did not adopt an adequate risk-based approach to the exercise of its supervisory functions, which needed to be informed by risk assessments carried out
  - » Failed to base the frequency and intensity of its onsite and off-site supervision on the risk profiles prepared
  - » Failed to regularly review Members' risk profiles as required by Regulation
- During the Suspension Period, 17 October 2022 to 26 July 2023:
  - » Failed to keep a record in writing of the actions it has taken in the course of its supervision, and of its reasons for deciding not to act in a particular case
  - » Failed to take appropriate measures to review the adequacy of the policies, controls and procedures adopted by relevant persons and the way in which those policies and controls had been implemented

FINTRAIL

FINTRAIL is a **global financial crime consultancy** comprising experts from the very industries we support. From strategy to execution, we help you build and maintain controls that **protect your customers and your bottom line.** Our services cover every stage of your compliance journey—ensuring you stay one step ahead.

Find out more

End-to-end support **for your financial crime compliance programme**

1

Risk Assessment & Programme Design

Customer risk assessments; policy and procedure design

2

Control Implementation

Screening (sanctions, PEPs, adverse media); transaction monitoring controls optimisation

3

Training and Awareness

Bespoke, trainer-led sessions designed in-line with your requirements

4

Testing and Assurance

Independent audits (AML, fraud, sanctions and more); targeted assurance and health checks

5

Remediation and Continuous Improvement

Remediation and regulatory enforcement support

We are a consultancy with expertise in using financial and regulatory technology to combat financial crime.