FINTRAIL
A COSEGIC COMPANY

Q2 2026

REGCAP

A summary of the latest FinCrime regulatory news

www.fintrail.com

contact@fintrail.com

Contents

Global news 3
UK 5
European Union 10
North America 13
Asia 16

Global news



Financial Action Task Force plenary

The Joint Financial Action Task Force (FATF) Plenary concluded on 19 June. Bosnia and Herzegovina and Iraq were added to FATF's List of Jurisdictions under Increased Monitoring (the 'grey list'), whilst Algeria and Namibia were removed.

The plenary also marked the conclusion of the Mexican presidency of FATF. Under the incoming UK presidency, FATF plans to pursue a step up in the international response on fraud, strengthening implementation of the risk-based approach, and enhanced information sharing practices.

What this means - With the amendments to the UK Money Laundering Regulations having taken effect in June 2026, firms are no longer required to apply Enhanced Due Diligence (EDD) solely because a country appears on the FATF grey list. However, firms must continue to assess and mitigate the financial crime risks associated with customers, products, and services connected to those jurisdictions. In particular, firms operating across multiple jurisdictions should review and, where necessary, update their country risk assessment frameworks. This is especially important where regulatory lists diverge; for example, the EU's list of high-risk third countries does not currently include Iraq or Bosnia and Herzegovina.

FATF launches public consultation on guidance to increase payment transparency

FATF has launched a consultation on draft guidance for implementing strengthened cross-border payment transparency under Recommendation 16. R16 was itself revised in June 2025 with a view to adding a 'critical safety net to the international payment system by increasing transparency of information that accompanies cross-border payments and requiring the introduction of tools to protect against fraud and error'. All countries are currently expected to fully implement these changes by the end of 2030. Specific areas of this consultation include detecting and preventing misdirected payments, application to newer payment methods, financial inclusion (particularly in lower-capacity jurisdictions), and meeting data privacy requirements. **Stakeholders have until 21 August 2026 to respond.**

What this means - Firms whose services involve cross-border transfers of funds need to be aware of the role they play in the payment chain and the incoming expectations regarding end-to-end transparency. Whilst FATF's target of 2030 might seem like some time away, some firms may need to make significant technological changes to align with the revised R16.

The Wolfsberg Group updates its guidance on the risk-based approach

The Wolfsberg Group has refreshed its guidance on the risk-based approach, emphasising **proportionality, prioritisation and effectiveness**, concluding that "a focus on everything is a focus on nothing".

Proportionality: there is no 'one-size-fits-all' approach, and a firm's controls should be aligned to its business model, customer base, geographic reach and risk appetite. This should be informed by its assessment of the risks the firm is exposed to.

Prioritisation: resources should be deployed to the highest risks which the firm is exposed to, which may entail 'stopping, reducing and/or redesigning existing measures that are determined to be redundant, duplicative or unproductive'.

Effectiveness: a firm should demonstrate effective outcomes, rather than a rules-based, tick-box approach. The Wolfsberg Group emphasises that this allows for a more 'responsive, forward-looking and dynamic approach to risk management'.

What this means - regulators and auditors will increasingly demand proof that compliance frameworks are proportionate and effective in managing financial crime risks; firms should ensure that their strategies, investments and areas of focus are risk-based and are yielding tangible results.

Egmont Group Marks International FIU Day on 9th June, reinforcing the importance of collaboration

The Egmont Group, a global network of Financial Intelligence Units (FIUs) celebrated International FIU day on 9 June, recognising the critical role of FIUs in safeguarding the financial system. In their statement, Egmont Group have highlighted the evolving financial crime landscape and challenges faced by FIUs, shaped by 'technological change, global connectivity and increasingly sophisticated criminal networks', and how the need to strengthen cooperation, nationally, regionally and internationally is critical to fighting financial crime. The Egmont Group will convene its 32rd Plenary meeting in Azerbaijan from 5-10 July 2026, which will include a thematic session focused on strengthening public-private partnerships.

UK

Updates to the UK Money Laundering Regulations

The Money Laundering and Terrorist Financing (Amendment) Regulations 2026 came into force on 30 June 2026, introducing a series of targeted amendments to the UK's Money Laundering Regulations(MLRs). The changes are intended to simplify certain requirements, reinforce the risk-based approach, and address areas where the existing rules have led to unnecessary complexity.

Some of the key changes include:

- Sterling replaces euro thresholds – various monetary thresholds throughout the MLRs have been converted from euros to pounds sterling.
- A more proportionate approach to Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) – The amendments refine CDD and EDD requirements, giving firms greater flexibility to apply a genuinely risk-based approach. This includes changes to EDD triggers for high-risk jurisdictions, which are now linked to the FATF Call for Action list (the 'black list') rather than the 'grey list'. It also includes clarification around what constitutes an "unusually complex or unusually large" transaction.
- New requirements for pooled accounts – Firms offering pooled accounts must now take additional steps to understand how the account will be used, assess the associated ML/TF risks, and implement appropriate controls.
- Cryptoasset firms – New EDD requirements will apply to cross-border correspondent relationships involving cryptoasset exchange providers and custodian wallet providers, although these provisions come into force in 2027.

What should firms do?

Although many of the changes are incremental, firms should review and update their AML policies, procedures, risk assessments and training materials to ensure they reflect the revised requirements. In particular, organisations should consider whether their CDD and EDD procedures, transaction monitoring guidance and jurisdictional risk assessments continue to align with the updated regulations and the UK's evolving risk-based approach. Firms offering pooled accounts should pay particular attention to the new requirements and assess whether their current controls are sufficient. Cryptoasset firms should begin preparing for the correspondent relationship EDD requirements coming into force in 2027, rather than treating these as a future concern.



The UK government launched a call for evidence seeking views on how information is currently shared in detecting, investigating, disrupting and preventing economic crime. The exercise will focus on identifying legal, cultural and operational barriers that prevent effective data sharing, and will look for ways to strengthen and reform the existing system.

The review will cover all economic crimes including money laundering, fraud and corruption. The consultation period has closed.

Also on the topic of information sharing, the FCA's Market Watch 85 covers how the Economic Crime and Corporate Transparency Act (ECCTA) can help firms legally share customer data to prevent economic crime. The ECCTA allows regulated firms to share customer information to prevent, detect and investigate economic crime protecting firms against civil liabilities or breaches of confidentiality.

What this means: Firms should familiarise themselves with the existing powers available under the ECCTA to share customer data for the purpose of preventing and detecting economic crime. Where firms are not already leveraging these provisions, now is a good time to assess whether information sharing arrangements could strengthen their financial crime controls — particularly in relation to fraud and money laundering detection. Legal and compliance teams should ensure that any data sharing is properly documented and falls within the scope of the protections the ECCTA provides.

The FCA has conducted a multi-firm review of CDD, EDD and ongoing due diligence against regulatory requirements and expectations. The review highlights good and poor practices and is part of the FCA's wider supervisory work.

Good practices identified include firms having clear differentiation between CCD and EDD procedures, senior management involved in the EDD escalation procedures, and using third parties to review CCD and onboarding procedures annually.

Poor practices include poor quality risk assessments, weak oversight of automated processes, failure to follow internal policies and procedures when conducting periodic reviews and having poor record keeping of EED undertaken.

What this means: Firms should use the FCA's findings as a practical benchmark against which to assess their own CDD and EDD arrangements. In particular, firms should review the quality of their customer risk assessments, the robustness of oversight over any automated processes, and whether periodic review processes are being followed consistently in practice, not just documented in policy. Poor record keeping of EDD undertaken is a specific area of concern flagged by the FCA and one that is straightforward to address with the right controls and culture in place.

The FCA publishes a multi-firm review of Insurance financial crime controls

The FCA has published the findings of its multi-firm review of insurers' financial crime controls. While the regulator concluded that most firms have broadly effective systems and controls in place, the review demonstrates an expectation for greater precision and granularity in a sector traditionally regarded as presenting lower financial crime risk.



Key findings include:

- **Enterprise-wide risk assessments should accurately reflect the firm's business model** and capture the specific financial crime risks associated with different business lines, such as life insurance, wholesale broking, retail distribution and delegated authority arrangements.
- **Policies and procedures should be appropriately tailored** to individual legal entities, jurisdictions and business units, rather than relying heavily on group-wide frameworks
- **Financial crime controls should be proportionate**, well justified and supported by documented rationale explaining why particular controls are, or are not, appropriate for the firm's business model
- **Firms should strengthen governance** by clearly defining roles and responsibilities, demonstrating structured control testing, and maintaining effective oversight of outsourced activities
- **Firms should avoid over-reliance** on contractual arrangements and ensure robust oversight of third-party service providers.

What this means for firms: Firms should use the FCA's findings as an opportunity to assess whether their financial crime framework would withstand regulatory scrutiny. FINTRAIL has published a blog summarising the review's key findings and outlining the practical steps insurance firms should consider to strengthen their financial crime controls.

The FCA is inviting stakeholders to share examples of good and poor AI practices within UK financial services. Through the Input Zone, the regulator wants to understand what "good" looks like in terms of safe and responsible AI development. The initiative



aims to build a clearer picture of how AI can be developed and deployed safely and securely while supporting growth and innovation across the sector.

The insights gained will be used to publish a good and poor practices guide, which will be published later this year. **Stakeholders have until 19 June 2026 to submit their response.**

What this means: Firms using or developing AI tools within their financial crime or wider compliance functions should consider whether to engage with the FCA's Input Zone process. Contributing examples of good and poor practice helps shape the regulatory framework that will ultimately govern AI use across the sector. Regardless of whether firms choose to submit, the forthcoming good and poor practices guide is likely to be a significant reference point for supervisory expectations, firms should monitor its publication and assess their own AI arrangements against it when it is released.

The UK's Crown Prosecution Service has published its Serious and Economic Organised Crime Strategy aimed at curbing serious crime. It is estimated that financial crime costs the UK at least £47bn annually. Due

to fraudsters and criminal groups turning to "poly-criminality" often linking to cybercrime and human trafficking, CPS will be taking a more forceful, proactive approach. This will involve early prosecutorial engagement, investing in new technologies such as AI, increased staffing levels and confiscating criminal proceeds.

What this means: The CPS's shift towards earlier prosecutorial engagement and greater use of technology signals a more assertive approach to economic crime enforcement. Firms should ensure that their suspicious activity report (SAR) processes, fraud controls and liaison with law enforcement are sufficiently robust to support this direction of travel. The explicit link to poly-criminality — where financial crime intersects with cybercrime and human trafficking — is a reminder that firms should be reviewing whether their transaction monitoring and risk assessment frameworks adequately capture these converging typologies.

Nationwide has introduced a "Hide Reference" feature on its platform, allowing users to block payment reference text. Abusers could previously use the payment reference text to send hurtful messages to their victims (e.g. while paying child support or maintenance). This feature gives control back to victims, ensuring these messages never reach them. This follows Starling's successful rollout of the same feature in 2023. Nationwide calls on other firms within the industry to follow suit.

What this means: This development is primarily of relevance to firms offering retail payment services. Firms should consider whether similar controls could be implemented within their own platforms to protect vulnerable customers from financial abuse conducted through payment references. Beyond the immediate product question, this is a useful prompt to review whether financial abuse and domestic abuse are adequately addressed within fraud and vulnerability frameworks more broadly.

UK Finance in partnership with Shelter, has launched an expanded pilot programme that aims to improve people's access to bank accounts. Building on Shelter's successful "Breaking the Cycle" scheme, the programme aims to help people who do not have a standard ID or proof of address, who often face barriers when opening an account.

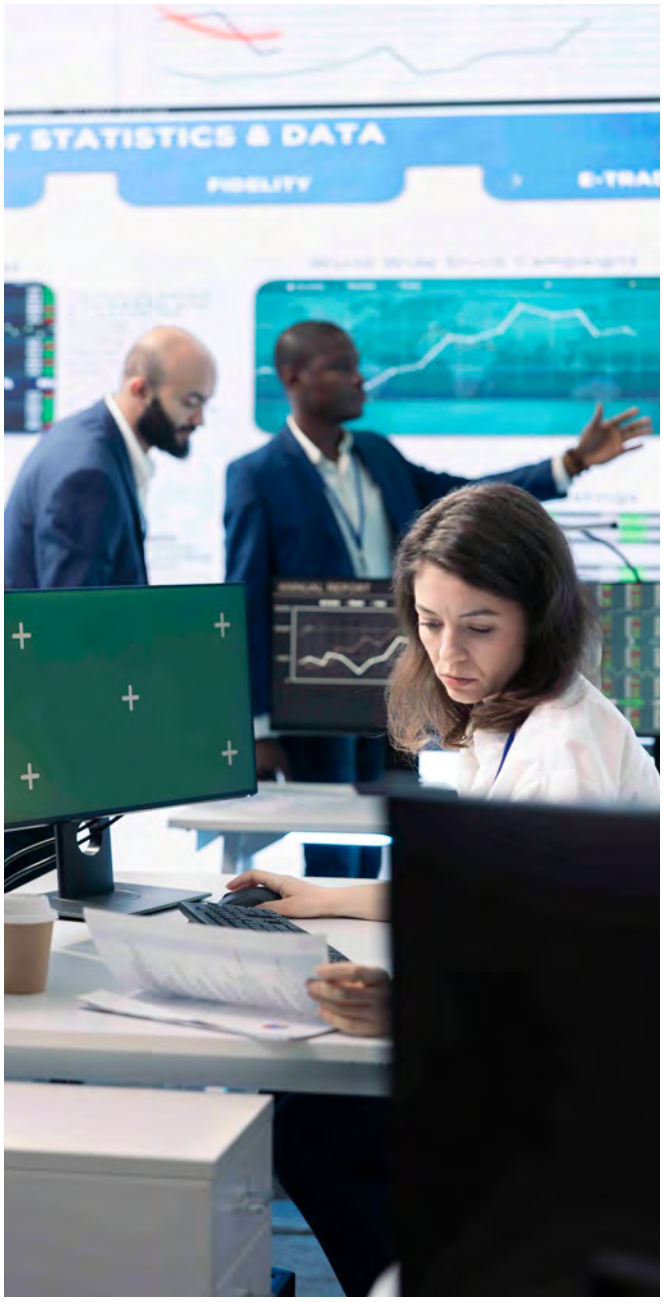
What this means: Firms should be aware of this initiative as it relates to the practical application of CDD requirements for customers who lack standard documentation. The pilot is a reminder that financial inclusion and AML compliance are not mutually exclusive — firms can take a proportionate, risk-based approach to ID verification for vulnerable customers without compromising their obligations. Firms should review whether their CDD policies provide sufficient flexibility and guidance for staff dealing with customers who cannot provide conventional forms of identification.



On 4th June 2026, the FCA required Euro Exchange Securities UK Limited (EES) — an electronic money and payment services firm — to immediately cease all regulated activity. The same day, the Court appointed interim managers from Teneo Financial Advisory to take control of the firm's affairs. The FCA identified concerns across three areas: systemic weaknesses in EES's financial crime framework, inadequate safeguarding arrangements and problems with its ownership and governance structure. The FCA considers these issues to pose a risk to both consumers and market integrity.

What this means: This is a notable escalation of FCA enforcement in the payments and e-money sector. The combination of a halt to all regulated activity and court-appointed interim managers rather than a fine or remediation plan signals that the FCA considered the risks serious enough to require immediate intervention rather than a managed wind-down. The explicit mention of ownership and governance alongside financial crime weaknesses suggests concerns went beyond technical compliance failures. For payment institutions and e-money firms more broadly, this is a reminder that the FCA is willing to act swiftly and decisively where it identifies systemic AFC deficiencies, and that safeguarding and governance are treated as equally important as the





European Union

The European Parliament's Economic Governance and EMU Scrutiny Unit (EGOV) has produced a briefing comparing differing AML frameworks across major financial jurisdictions. Evaluating the USA, EU, the UK, Japan and Singapore, the review aims to understand how differing institutional designs impact the effectiveness and enforcement of financial crime supervision.

The briefing highlights that differences in regulations and supervision can create opportunities for money laundering to occur and that financial crime prevention needs clear data and international co-operation to be fully effective.

What this means: For firms operating across multiple jurisdictions, this briefing reinforces the importance of not assuming that compliance with one regime translates to compliance with another. Differences in regulatory frameworks and supervisory approaches can create gaps that are exploited by those seeking to launder money. Firms should ensure that their group-level financial crime frameworks are sufficiently flexible to account for jurisdictional divergence, and that local compliance teams have clear visibility of where their obligations differ from the group baseline.

France

The French Prudential Supervision and Resolution Authority (ACPR, Autorité de Contrôle Prudentiel et de Résolution) and the French FIU Tracfin have published a report on the use of virtual IBANs (vIBANs) in France. While the report highlights that the majority of uses are for legitimate purposes around payment reconciliations, analytical accounting and treasury management, it also highlights financial crime risks. Using multiple secondary vIBANs linked to different countries can create the impression of a domestic transaction, even though funds flow across borders. This can be used by money launderers as it complicates traceability, making it harder for law enforcement to investigate and prevent abuses.

European regulatory reforms coming into force in July 2027 will help reduce the risks, notably by improving their registration in bank account registers such as the French FICOBA database. However, ACPR and Tracfin also call on the International Organization for Standardization (ISO) to enhance the ISO 13616-1 standard in order to distinguish IBANs from vIBANs more clearly, particularly in cases involving redirection from one country to another.

What this means: Firms that issue or accept payments via virtual IBANs should review whether their transaction monitoring and KYC controls adequately account for the specific risks these instruments present. In particular, firms should consider whether their systems can identify when a vIBAN is being used to obscure the cross-border nature of a transaction, and whether their customer risk assessments flag this as a relevant factor. Firms operating in France should also monitor the regulatory developments anticipated for July 2027 and begin assessing what operational changes may be required.

Europol's Internet Organised Crime Threat Assessment (IOCTA) report highlights how agentic and generative AIs, residential proxies and end to end encryption are accelerating and enabling organised cybercrime.

Ransomware is still a key tool of cybercriminals with over 120 active brands as of 2025. Scammers are moving away from

an extortion model towards data leaks. Also there is a growing use of state-backed actors using criminal networks for distributed denial of service (DDOS) attacks.

With cybercriminals using SIM box farms to bypass KYC checks, AI to create personalised scams and crime as a service (CaaS) to outsource scamming, online fraud schemes (OFSs) are now the fastest growing area of organised crime.

Cryptocurrencies, privacy coins, decentralised exchanges and Neobanking with their very quick onboarding, transfers and weak AML controls are key ways criminals launder money.

What this means: Firms should review whether their fraud, cybercrime and AML controls adequately reflect the threat landscape described in the IOCTA report. The increasing use of AI by criminal networks to personalise scams, bypass KYC checks and automate fraud at scale has direct implications for onboarding, transaction monitoring and customer authentication controls. Firms in the payments and crypto sectors in particular should assess their exposure to crime-as-a-service models and ensure that their risk assessments, transaction monitoring configurations and typology libraries are kept current with these developments.

AMLA consultations

Consultation on the draft Guidelines on business-wide risk assessment:

AMLA held a consultation on the draft guidelines on business wide risk assessments (BWRAs) under Article 10.4 of Regulation 2024/1624. The consultation was open to all stakeholders who have an interest in the EU's AML/CFT framework. The draft guidance proposes four minimum requirements that would be applied to all Obliged Entities, and stresses the importance of firms taking ownership of their BRWAs, ensuring it is proportionate to their firm's individual risk and complexity. The consultation is now closed.

What this means: Firms operating within the EU's AML/CFT framework should review the draft AMLA guidance against their existing BWRA processes to identify any gaps ahead of the finalised guidance coming into force. In particular, firms should assess whether their BWRAs can demonstrate genuine proportionality to their individual risk profile, rather than relying on generic or templated approaches. Given the overlap with similar expectations from the FCA and Virtual Assets Regulatory Authority (VARA) in Dubai, firms operating across multiple jurisdictions may wish to use this as an opportunity to align their risk assessment frameworks more broadly.

Consultation on the draft Guidelines on ongoing monitoring of a business relationship:

AMLA has launched a consultation on its draft guidelines under Article 26(5) of Regulation (EU) 2024/1624. The guidelines aim to promote a consistent approach across financial and non-financial entities to maintaining up-to-date customer information and monitoring for suspicious activity. They reinforce the importance of ongoing monitoring as a core element of an anti-financial crime framework, requiring firms to continuously assess customer activity and transactions for unusual or suspicious behaviour throughout the business relationship. The consultation is open until 3 September 2026.

What this means: Firms subject to the EU AML framework should review their ongoing monitoring policies and procedures to ensure they support continuous, risk-based monitoring of customer activity throughout the lifecycle of the business relationship. Firms that wish to provide feedback on the draft guidelines can submit responses until 3 September 2026.

TheEUcouncilhaspublishedDocument 8222/26, the final compromised text for a new Payment Services Directive 3 (PSD3). The proposal aims to modernise and harmonise the EU's payments framework in response to the rise of digital payments and regulatory inconsistencies.

Among other things, the Directive will bring electronic money tokens and crypto-assets providers in line with MICA rules, which will force firms to have strong and effective AML and CTF policies and procedures in place when seeking authorisation.

What this means: Firms operating in EU payments markets — including e-money institutions, payment institutions and cryptoasset service providers — should begin assessing how PSD3 will affect their authorisation requirements, AML obligations and product frameworks. The alignment of electronic money tokens and crypto-assets with MiCA rules is a significant development for the sector, and firms should not wait for final implementation to begin their gap analysis. Compliance, legal and product teams should work together to understand the implications across licensing, controls and customer journeys.





North America

USA

The US Treasury proposes rule to implement the GENIUS Act's requirements to counter illicit finance

The US Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Assets Control (OFAC) have issued a joint proposed rule to implement provisions of the Guiding and Establishing National Innovation for US Stablecoins Act (GENIUS Act). This rule promotes innovation in payment stable coins whilst requiring permitted payment stablecoin issuers (PPSIs) to 'adopt and maintain an effective sanctions compliance program as required by the GENIUS Act'. The proposed rule would require PPSIs to, among others, establish and maintain AML/CFT programs and to comply with standard record keeping and reporting requirements under 31 CFR part 501. **Industry is invited to comment on the proposed rule by 9 June 2026.**

What this means: PPSI firms operating in the US should review the proposed requirements to understand their potential compliance obligations. In particular, firms should assess whether their AML/CFT and sanctions compliance frameworks, governance arrangements and record keeping processes would meet the proposed standards.

The Financial Crimes Enforcement Network (FinCEN) has proposed significant reforms to AML/CTF rules under the Banking Secrecy Act (BSA). The changes would require firms to establish and maintain effective risk based AML/CFT policies and procedures and allocate greater resources to the supervision of high-risk customers. US firms must have a US based AML/CFT officer who would be responsible for the day to day monitoring and compliance with BSA rules. Finally FinCen's AML/CFT supervision and enforcement powers will be expanded and will work more closely with federal banking regulators.

What this means: US-facing firms and those with operations or customers in the United States should monitor these proposed reforms closely as they move through the rulemaking process. The proposed requirement for a US-based AML/CFT officer and the expansion of FinCEN's supervisory and enforcement powers signal a more demanding compliance environment ahead. Firms should assess whether their current governance arrangements, resourcing and risk-based controls would meet the proposed standards, and begin addressing any gaps proactively.

FinCEN has issued FIN 2026 Alert002 to assist financial institutions in identifying actors suspected of funding and procurement networks for the Islamic Revolutionary Guard Corp (IRGC). The IRGC are using multi-jurisdiction shadow banking, layered corporate structures and digital assets to launder the proceeds from selling sanctioned Iranian oil, which totalled over $4billion in 2025.

FinCEN identified irregular shipping documentation, efforts to disguise oil origins and unclear sources of funds as some potential red flag indicators that firms should be aware of.

What this means: Firms with exposure to trade finance, commodities, shipping or correspondent banking should review their controls against the red flags identified in the FinCEN alert. In particular, firms should assess whether their transaction monitoring scenarios and sanctions screening are calibrated to detect irregular shipping documentation, attempts to obscure the origin of funds or goods, and the use of layered corporate structures and digital assets associated with sanctions evasion. The use of multi-jurisdiction shadow banking by the IRGC is a specific typology that firms with cross-border payment flows should factor into their risk assessments.

FinCEN has issued a warning to financial institutions to remain vigilant and lookout for signs of human trafficking linked with the FIFA World Cup. FinCEN warns that major events can create a concentrated demand of illicit services and vulnerable people may be used for sex or labour exploitation.

Firms are strongly encouraged to notify law enforcement of suspected trafficking and that customer facing staff must know and be able to identify transactional and behavioural indicators that may indicate human trafficking may be occurring.

What this means: Firms with exposure to hospitality, travel, payments or cash-intensive sectors in or around World Cup host cities should ensure that their customer-facing staff are trained to identify the behavioural and transactional indicators of human trafficking set out in the FinCEN warning. Transaction monitoring scenarios should be reviewed to assess whether they would flag relevant patterns of activity. Firms should also confirm that their internal escalation and SAR filing processes are clear and operable for this specific typology, and that any suspicious activity is reported to law enforcement promptly.

Canada

Canada has introduced a much tougher AML enforcement regime, significantly strengthening FINTRAC's ability to penalise non-compliant firms. Under the new framework, which applies to violations occurring from 26 March 2026, the maximum administrative monetary penalties have increased by up to 40 times (with very serious violations now attracting penalties of up to C$20 million). FINTRAC has also gained new enforcement tools, including mandatory compliance agreements and compliance orders, and can now take a firm's ability to pay into account when determining penalties. The changes send a clear signal that Canada is moving towards a more assertive supervisory approach, with greater expectations on firms to demonstrate robust, effective AML compliance programmes.

What this means: Firms operating in Canada or with Canadian regulatory obligations should treat this as a significant shift in the enforcement environment. The increase in maximum penalties — up to C$20 million for very serious violations — combined with new enforcement tools such as mandatory compliance agreements and compliance orders, means that the cost of non-compliance has risen materially. Firms should review the robustness of their AML compliance programmes against FINTRAC's expectations and prioritise any known gaps as a matter of urgency.

FINTRAC has published a special bulletin on money laundering associated with extortion against Canada's South Asian diaspora.

Victims are often small to medium sized business owners in sectors like transportation, retail, construction or hospitality. Criminals often identify themselves as being part of the Lawrence Bishop Network, a designated terror gang within Canada. Victims are often described being threatened, intimidated or shot at if their demands are not met.

Criminals often demand payment through money transfers, cheques, cash deliveries or cryptocurrencies. As part of Operation TAPEX, FINTRAC urges reporting entities to be on the look out for suspicious transactions and submit SARs using the term #TAPEX if they reasonably suspect the transaction is linked to money laundering or extortion.

What this means: Firms with exposure to the Canadian market — particularly those serving small and medium-sized businesses in transportation, retail, construction or hospitality — should ensure that their transaction monitoring and SAR processes are calibrated to detect the payment typologies described in the bulletin. Staff should be made aware of Operation TAPEX and the requirement to include #TAPEX in SAR filings where a transaction is reasonably suspected to be linked to this activity. Customer-facing teams should also be sensitised to the indicators that a customer may





Asia

Singapore

FATF and the Asia Group on Money Laundering (APG) have conducted a mutual evaluation reviewing Singapore's AML, CFT and proliferation financing measures, assessing whether they are fit for purpose and what upgrades are needed to meet emerging challenges. The assessment found that Singapore's financial crime needs are being met by an effective, competent and co-ordinated regime that is willing to experiment with new techniques to prevent crime.

While the report praises Singapore's fight against financial crime, it highlights that the AML, CFT and proliferation financing systems must be able to demonstrate consistent risk based results. In the last 5 years, 80% of money laundering investigations were initiated by victims, suggesting that Singapore is not able to investigate or search for less visible forms of money laundering or financial crime.

What this means: For firms with operations or correspondent relationships in Singapore, the mutual evaluation provides useful context on the maturity and effectiveness of Singapore's AML regime. The finding that 80% of money laundering investigations were initiated by victims — rather than proactively identified by authorities — is a notable gap, and one that reinforces the importance of robust transaction monitoring and SAR filing by regulated firms operating in the jurisdiction. Firms should not assume that a strong regulatory environment removes the need for their own proactive financial crime controls.

UAE

The UAE has issued a report addressing the findings and importance of the 2024 National Risk Assessment (NRA). The report reinforces the Economic Ministry's commitment to strengthening AML, CFT and CPF across Designated Non-Financial Businesses and Professions (DNFBPs). DNFBPs include casinos, real-estate, precious metal dealers and professional services (e.g. lawyers or accountants), sectors that are more susceptible to financial crime.

The review sets out clear guidance expectations for supervised entities and provides practical guidance for DNFBPs to adopt a risk based approach and align them with national priorities and industry controls. What this means: Firms operating in the UAE or with significant customer or transaction exposure to the UAE should review the NRA findings and assess whether their own risk frameworks adequately reflect the risks identified — particularly in relation to DNFBPs and the sectors highlighted as more susceptible to financial crime. Where firms rely on professional service providers, real estate agents or other DNFBP counterparties in the UAE, their due diligence and ongoing monitoring of those relationships should be reviewed in light of the NRA's findings.

Dubai's Virtual Assets Regulatory Authority (VARA) has published new AML/CFT Business Risk Assessment (BWRA) Guidance that raises the bar for how firms are expected to maintain and evidence their financial crime risk assessments. Drawing on best practice identified through a recent thematic review, the guidance requires VASPs to review and update their BWRAs at least every three months, explicitly consider separate risks relating to money laundering, terrorist financing, proliferation financing and sanctions, and demonstrate that they have considered authoritative sources such as the UAE National Risk Assessment, FATF and MENAFATF publications, and UAE FIU strategic analysis whenever these are updated. It also

highlights emerging risks including AI, anonymity-enhancing transactions and crowdfunding.

What this means: Virtual asset service providers regulated by VARA should treat this guidance as a significant uplift to their risk assessment obligations. The requirement to review and update BWRAs at least every three months is considerably more frequent than most firms' current practice, and firms should assess whether their existing processes and resourcing can support this cadence. The explicit requirement to consider ML, TF, proliferation financing and sanctions risks separately — and to draw on authoritative sources including the UAE NRA and FATF publications — should be reflected in BWRA methodology documentation. Firms should also ensure that emerging risks including AI, anonymity-enhancing transactions and crowdfunding are addressed within their assessments.

The UAE Financial Intelligence Unit (UAEFIU) has published a report on different types of modern slavery and human trafficking, and how money laundering links back to key patterns, behaviours and risks associated with slavery and human trafficking.

The report highlights how sexual and labour exploitation are often linked to vulnerable groups and the important role banks and payment institutions have in detecting and preventing these crimes. To assist in the prevention of these acts, the report provides practical risk indicators, designed to help firms detect, prevent and improve data quality to assist authorities.

What this means: Firms operating in the UAE — particularly banks and payment institutions — should review the risk indicators published by the UAE FIU and assess whether their transaction monitoring scenarios and CDD processes are calibrated to detect the patterns associated with modern slavery and human trafficking. The report's emphasis on data quality as a tool for assisting authorities is a prompt for firms to review the completeness and accuracy of the information they capture at onboarding and during the course of the customer relationship.





Thematic Focus: Fraud

Fraud losses rise despite better victim reimbursement

Recent reports from UK and European regulators show that while victims are being reimbursed more effectively, fraud continues to grow in scale and sophistication.

The UK's Payment Systems Regulator (PSR) reported that 89% of APP fraud losses in scope were reimbursed in 2025, up from 65% previously. However, around 3% of claims were rejected because customers were deemed not to have met the required standard of caution.

However, UK Finance reported in their 2026 Annual Fraud Report that criminals stole £1.28 billion through fraud in 2025 across 4.06 million cases, increases of 4% and 11% respectively. £576 million was stolen through APP fraud, an increase of 19%, and within that, Investment scam losses reached a record £220 million, up 40% year-on-year. The report highlights the increasing use of AI-enabled impersonation and social engineering scams.

Similar concerns were identified by Netherland's Central Bank, De Nederlandsche Bank (DNB), which found that 10% of people aged 15 and over in the Netherlands were victims of online fraud or scams in 2025. The regulator warned that criminals are increasingly using AI and called for greater collaboration between banks, payment firms and online platforms.

What this means: Firms should:

- Ensure that fraud risk assessments address emerging threats such as AI-enabled scams to keep pace with evolving criminal tactics;
- continue to invest in consumer awareness and scam education programmes, helping to deliver the right messages, to the right people, in the right way.

CIFAS publishes fraud trends research

The UK's fraud prevention service Cifas has published its Workplace Fraud Trends, which found that 13% of employees have either sold their company login details to a former colleague or know someone who has. While 75% said this is completely wrong, attitudes varied by seniority. One-third of senior managers, 42% of C-suite executives, and 81% of business owners said selling logins can be justified. This suggests acceptance

increases at higher levels of an organisation. Selling company login details can help criminals commit fraud, launch cyberattacks, or access sensitive business information.

What this means: firms should ensure that their fraud risk assessment considers insider threats, including the misuse of sale of company credentials. Firms should assess the effectiveness of controls such as access management, user monitoring, segregation of duties, employee screening and offboarding processes.

FinCEN Issues guidance to help financial institutions share fraud data

FinCEN has updated its guidance to make it clearer how financial institutions, including money services businesses, can share information about suspected fraud with each other under Section 314(b) of the USA PATRIOT Act.

Section 314(b) allows financial institutions to exchange information under a legal safe harbor that protects them from liability. This helps them identify and report potential money laundering, terrorist financing, and related suspicious activities.

Participation is voluntary. To take part, institutions must register through FinCEN's Financial Industry Portal and take reasonable steps to confirm that the other institution they are sharing information with is also registered under Section 314(b).

What this means: US-facing firms and money services businesses should review the updated FinCEN guidance and assess whether they are making full use of the Section 314(b) framework. The legal safe harbor it provides is a meaningful protection that removes one of the most commonly cited barriers to information sharing which is liability risk, firms that are not yet registered or are not actively using the mechanism should consider whether it could strengthen their fraud and AML detection capabilities. Participation is voluntary, but the direction of travel from regulators globally is clearly towards greater information sharing as a collective defence against fraud and financial crime. Firms that build the operational and governance frameworks to support this now will be better positioned as expectations in this area continue to rise.





HSBC Australia fined for significant failures in its scam protection controls

The Federal Court of Australia has fined HSBC's local subsidiary AU$35 million (£18.5 million) for failures in its scam protection controls. The Australian Securities and Investment Commission (ASIC) chair described this fine as the "strongest scam wake-up call yet" for the industry. HSBC was found to have inadequate controls on its internal transfer system exposing customers to the risk of unauthorised payments, and to have breached its obligations under the ePayments Code by taking on average 4-months to finalise cases.

What this means: Firms should ensure that scam protection is treated as an operational discipline with clear ownership., measurable outcomes and regular assurance activity, not simply as a policy commitment. A four month average to finalise cases is the kind of operational failure that regulators are increasingly unwilling to tolerate, firms should assess whether their current SLAs, resourcing and case management processes would withstand similar scrutiny.

Trio of Spanish banks launch 'FrauDfense'

Three of Spain's largest banks – Banco Santander, BBVA and CaixaBank – have launched a new joint anti-fraud service through their shared venture, FrauDfense. The platform, known as FrauDfense Check, is designed to prevent fraud before it occurs by enabling the secure exchange of fraud-related information between participating financial institutions. The initiative promotes greater industry collaboration and positions the Spanish banking sector as a leader in collective fraud prevention. The banks also noted that the model will help institutions prepare for upcoming requirements under the EU's revised Payment Services Regulation (PSR), which will require payment service providers to share fraud-related information with one another to strengthen fraud detection and prevention.

What this means: The FrauDfense initiative is a practical example of what effective industry collaboration on fraud prevention can look like, and a signal of the direction of travel under the EU's revised Payment Services regulation. Firms should reflect on whether they are making full use of existing information sharing mechanisms with their own third-party providers, correspondent banks, payment partners and industry peers - not just within their own organisation. The upcoming PSR requirement to share fraud-related information will make this a regulatory obligation rather than a best practice. Firms that have not yet built the frameworks to support effective information sharing should begin doing so now.

Thematic Focus: Sanctions

FCA report on sanctions systems and controls:

The FCA has published its assessment of regulated firms' sanctions systems and controls, highlighting good and poor practices and where firms need to improve to better support compliance with sanction rules. This report sets out the FCA's principal findings since their September 2023 report on firms' responses to increased sanctions.

Theme	Good Practice	Poor Practice
Governance & Oversight	Up-to-date sanctions policies, clear MLRO reporting, role-specific training, and regular audit assurance.	Policies focus only on asset freezes or lack oversight of group-provided sanctions services.
Management Information (MI)	Regular monitoring of high-risk customer exposure with quantitative and qualitative analysis.	Insufficient MI on overseas branches and sanctions compliance.
Risk Assessments	Assess financial, trade, and proliferation financing risks; identify and remediate control gaps.	Risks quantified without documented rationale or evidence.
Due Diligence & Ongoing Monitoring	Regularly updated CDD processes and risk-based customer review frequencies.	Poor oversight of outsourced CDD; inadequate EDD and monitoring for high-risk customers.
Screening Policies	Clear screening scope, governance, exclusions process, and mitigating controls.	Policies not embedded in practice; unjustified exclusions or reliance on outdated vendor settings.
List Management & Data Feeds	Use multiple data sources, enhanced watchlists, and robust vendor arrangements.	Limited understanding of list management and weak controls over list updates.

Calibration, Configuration & Testing	Effective fuzzy matching and regular validation/testing of screening systems.	Poorly calibrated systems and limited understanding of vendor screening logic.
Alert Management & Resourcing	Clear escalation procedures and quality assurance of investigations.	Missed SLAs, weak quality controls, and inadequate oversight of third-party screening providers.
Evasion Detection & Investigation	Training on sanctions evasion risks, proactive testing, lookbacks, and trade document checks.	Evasion risks not adequately reflected in risk assessments, controls, or procedures.
Asset Freezing & Licence Compliance	Clear account restriction, freezing, and licence compliance procedures.	Poorly documented freezing procedures and failure to consider freezing obligations during offboarding.
Reporting & Assessing Breaches	Clear breach reporting procedures and remedial action processes.	No specific poor practices identified.

What this means: Firms should ensure they have a clear understanding of their sanctions risk exposure and maintain effective systems and controls across all customer and transaction journeys. These controls should be subject to regular review to ensure they remain comprehensive, proportionate, and effective in mitigating sanctions-related risks.

Where gaps or weaknesses are identified, firms should take timely and appropriate remedial action to address them and strengthen compliance outcomes.

OFSI publishes its strategy for 2026-2029

In April 2026, the Office for Financial Sanctions Implementation (OFSI) set out its core objectives for 2026 to 2029, covering how it will evolve at pace over the next three years. The strategy paper marked ten years since OFSI's establishment to implement and enforce financial sanctions in the UK, and reflects on how it responded to challenges such as the Russian invasion of Ukraine in 2022.

The strategy aims to achieve three key outcomes:

- An enhanced understanding of threats and risks, grounded in data and evidence;
- High quality licensing and enforcement and focused compliance support in high-impact areas;
- Strong partnerships across government, the private sector and internationally.

The strategy is shaped around 4 key pillars: **Promote, Enable, Respond, Change** (PERC). Within this PERC framework, OFSI has committed to two new KPIs - that 50%

The OFSI PERC framework



Source: OFSI

of licencing cases will be completed within 6-months, and that 90% of enforcement investigations will be decided within 18-months.

What this means for firms: OFSI's commitment to publicly reported KPIs indicates a clear drive to accelerate investigations and enforcement outcomes. Firms should expect faster, more targeted investigations and should be prepared to respond

OFSI publishes a comparative view on the US and UK economic sanctions authorities

The OFAC-OFSI Enhanced Partnership was created to support private sectors to understand both sanctions regimes, particularly for firms operating cross-border. In June 2026, the US and UK jointly published guidance outlining key similarities and differences between the US Office of Foreign Assets Control (OFAC) and the UK's OFSI. The guidance deep dives into respective roles, responsibilities, definitions of key terms, and importantly, legal frameworks of each authority.

Some of the key similarities and distinctions include:

Theme	Good Practice	Poor Practice
List-based designations	The US operates under the Specially Designated Nationals and Blocked Persons list (SDN)	The UK uses the Sanctions List, which is maintained by HM Foreign, Commonwealth and Development Office
Restrictions on assets	OFAC "blocks" property	The UK "freezes" assets
Reporting requirements	Firms must report to OFAC following any holding, unblocking or transferring of blocked property within 10-days of taking that action (31 CFR §§ 501.603 and 501.604)	Firms must report to OFSI as described in regime-specific UK regulations. Most commonly, firms must report if they know or reasonably suspect that a person is a designated person, or has breached a prohibition, or failed to comply with an obligation. Firms can seek further guidance here.
Annual reporting	OFAC requires firms to submit an Annual Report of Blocked Property (ARBP) under 31 CFR §501.603 by 30th September each year.	OFSI requires firms to submit an Annual Frozen Asset Review by 30th November of each year.

Jurisdictional scope	The US enforces 'extraterritoriality' of Sanctions, for example, meaning that foreign branches and subsidiaries of US incorporated entities (i.e., those located outside of the US) must comply with OFAC sanctions	All individuals and entities in the UK must comply with OFSI, as well as activity within its territorial sea. This also includes foreign branches of legal entities incorporated or constituted under UK law.
Record keeping	Requirement to keep full and accurate records for at least 10-years after the date of the transaction (31 CFR §501.601)	The UK does not specify how long records should be retained for sanctions-related transactions, but firms should be prudent in retaining records for the purposes of making relevant records available to OFSI within a reasonable time frame
Permitted activities	This may entail exemptions or authorisations, such as general licences and specific licences	

The US publishes an OFAC introductory guide

In June 2026, the United States (US) published a new introductory guide to OFAC, aimed at helping private sector organisations better understand OFAC's sanctions framework and compliance expectations. The guide provides an accessible overview of the US sanctions regime and is intended as a practical resource for businesses that may be subject to OFAC's jurisdiction.

Among the topics covered are the fundamentals of how OFAC sanctions operate, the process for applying for specific licences, the procedures for seeking removal from an OFAC sanctions list, and OFAC's approach to sanctions enforcement. By bringing together these core concepts in a single reference document, the guide offers organisations greater clarity on how to navigate key compliance obligations and engage with OFAC where necessary.

What this means: These publications are particularly relevant for firms with a US nexus, including those operating in or with the US, transacting in US dollars, or dealing with US persons. It also provides a useful resource for organisations reviewing or updating their sanctions compliance framework, policies, and staff training materials as part of a broader policy refresh.

EU ruling on sanctions applicability

The European Union's Court of Justice has ruled that the mere inclusion of a customer's name on a third-country sanctions list does not automatically block the opening of a basic payment account. Rather, the person's inclusion on such a list should be treated as a risk indicator to be factored into a firm's assessment of the potential risk presented by entering into a relationship with such a customer. The outcome might still be a decision to decline or offboard, but the basis would be the firm's risk assessment, rather than the mere presence of a person on a particular sanctions list.

UK and EU Expand Russia sanctions measures

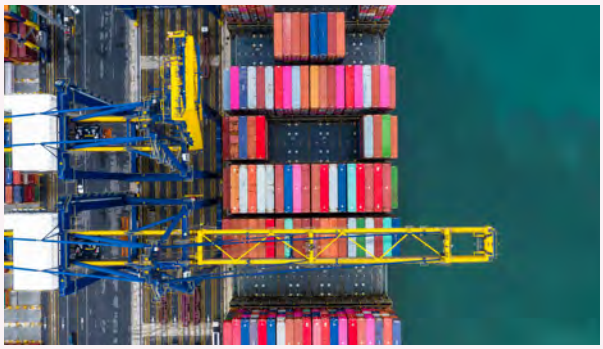
The UK and EU have continued to strengthen sanctions against Russia, with a growing focus on disrupting military supply chains, sanctions evasion networks, and alternative financing channels.

The UK imposed sanctions on 35 individuals and entities linked to Russia's drone production capabilities and recruitment networks supporting its war effort, including actors in third countries such as China and Thailand involved in supplying military goods.

Meanwhile, the EU adopted its 20th sanctions package against Russia, adding 120 new listings and expanding restrictions across the energy, military-industrial, shipping, and financial sectors. The measures also include a comprehensive ban on Russia-based crypto-asset service providers and platforms.

What this means: These developments highlight the increasing scope of sanctions regimes, particularly in relation to third-country intermediaries, military procurement networks, and digital financial infrastructure. Firms should ensure their sanctions controls, screening processes, and risk assessments remain aligned to these evolving requirements.





Penalties

Deutsche Bank AG London (DBLB) has been fined £165,000 by the Office of Financial Sanctions Implementation (OFSI) for breaches of the Russia (Sanctions) (EU Exit) Regulations 2019. The breaches related to Regulation 12, which prohibits making funds available to a person or entity owned or controlled by a designated person.

DBLB processed two payments totalling £635,618.75 to Okko LLC, a company wholly owned by JSC New Opportunities, an entity subject to UK financial sanctions. While OFSI recognised the benefits that third-party screening providers can offer, it emphasised that responsibility for sanctions compliance remains with the regulated firm. Firms must ensure that payments are screened effectively and that financial sanctions obligations are met, regardless of whether screening activities are outsourced.

What this means: Reliance on off-the-shelf screening solutions that are not appropriately configured, combined with weak governance and insufficient oversight, can significantly increase sanctions compliance risks. Regulated firms should have a detailed understanding of how their screening systems operate, including those provided by third parties, and implement regular testing, validation, and oversight to ensure sanctions-related alerts are generated and escalated appropriately.

Sabre Global Technologies Limited has been fined more than £1m for sanctions circumvention offences. SGT was fined for having made funds and economic resources available to a designated Russian airline for seven months in 2022, and tested alternative payment routes to get around UK sanctions. The penalty is the largest for financial sanctions breaches since Russia's 2022 illegal invasion of Ukraine, and also the first issued by OFSI for a circumvention offence under Regulation 19; this penalty comes as the UK steps up enforcement action on firms and individuals seeking to evade the UK sanctions regime.

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.