FINTRAIL

Q1 2026

REGCAP

A summary of the latest FinCrime regulatory news

www.fintrail.com

contact@fintrail.com

Global guidance

Financial Action Task Force plenary

The Joint **Financial Action Task Force (FATF)-MONEYVAL** Plenary concluded on 13th February. As a result, the following countries were added to FATF's List of Jurisdictions under Increased Monitoring (the 'Greylist'):

 Kuwait

 Papua New Guinea

In addition, following the plenary, the FATF has issued the following guidance and updates:

1. Ongoing monitoring of jurisdictions under increased monitoring

At this Plenary, the FATF added Kuwait and Papua New Guinea to the list of jurisdictions under increased monitoring.

2. Jurisdictions subject to a Call for Action

The FATF identifies countries or jurisdictions with serious strategic deficiencies in countering money laundering, terrorist financing, and proliferation financing. These jurisdictions are subject to a call for action (High-Risk Jurisdictions subject to a Call for Action - 13 February 2026) to protect the international financial system.

The FATF has updated its public statement on Iran, reaffirming that it remains a high-risk jurisdiction subject to a call for action due to significant deficiencies in its AML/CFT and proliferation financing regime.

The FATF continues to express concern over terrorist financing and proliferation financing risks, noting that Iran has made no material progress on its action plan. As a result, Iran remains on the FATF "black list" and the FATF calls on jurisdictions to apply enhanced due diligence and countermeasures, including restrictions on financial relationships and increased scrutiny of transactions linked to Iran.

3. Mutual Evaluations of Austria, Italy and Singapore

The Plenary discussed and adopted reports of the FATF mutual evaluations of Austria (led by the International Monetary Fund) and Italy, and the joint FATF-Asia-Pacific Group (APG) mutual evaluation of Singapore. These assessed the effectiveness of the countries' measures to combat money laundering, terrorist financing and proliferation financing, and compliance with the FATF Recommendations. The reports will be published in April – May 2026 following a global quality and consistency review.

The new, more risk-based assessments, place greater emphasis on countries' results in tackling money laundering, terrorist financing and proliferation financing. Under the new round of assessments, relevant countries will have a timebound Roadmap of Key Recommended Actions to strengthen the effectiveness of their defences against illicit finance within three years.

4. Tackling cyber-enabled fraud

The FATF approved a paper on cyber-enabled fraud which highlights the escalating fraud threat facing the globe, and the harm done to victims. As fraudsters continue to make use of digital innovations to accelerate the scale, speed, and complexity of fraud, partners across the anti-money laundering and countering terrorist financing and proliferation financing (AML/CFT/CPF) regime must also leverage innovative techniques to better prevent fraud, return victims' money and bring perpetrators to justice. Recognising these evolving threats, FATF has committed to focusing on fraud over the next few years.

What this means:

Firms should expect increased regulatory focus on fraud prevention, detection and recovery, with greater emphasis on using data, technology and cross-sector collaboration to combat increasingly sophisticated fraud typologies.

5. Virtual assets

As technology continues to evolve and in recognition of the inherently cross-border nature of virtual assets, the Plenary approved two new reports, to be published next month, that will help countries address emerging risks and support responsible innovation in finance.

A report on Understanding and Mitigating the Risk of Offshore Virtual Asset Service Providers (oVASPs) will explore risks associated with the unregulated provision of offshore VASP services. The report will look at how gaps and differences in regulatory and supervisory coverage are exploited by criminals and set out what governments can do to address this.

A Targeted Report on Stablecoins and Unhosted Wallets will examine emerging risks associated with stablecoins, which have grown rapidly in global scale, reach and importance in recent years. It makes recommendations to help countries and the private sector mitigate risks, including where stablecoins are being moved through peer-to-peer transactions.

What this means:

Firms should expect continued regulatory scrutiny on crypto-related activity, with a focus on cross-border risks, regulatory arbitrage, and controls around unhosted wallets and stablecoin flows, requiring stronger monitoring and risk management frameworks.

6. Setting the Strategic Priorities for 2026-2028

The Plenary set the FATF's Strategic Priorities for 2026–2028, focusing on evolving financial crime threats. Key areas include cyber-enabled fraud, risks from virtual assets (including stablecoins and unhosted wallets), mutual evaluations of countries' AML/CFT regimes, and strengthening global coordination with regional bodies. The priorities also highlight monitoring high-risk jurisdictions and emerging technology-driven risks, reinforcing the FATF's aim to ensure crime does not pay and to guide jurisdictions in adapting to increasingly sophisticated criminal methods. These priorities will be presented to FATF Ministers for endorsement at the upcoming April Ministerial meeting.

7. Cohesion across the Global Network

The Plenary agreed on a set of measures to increase FATF-Style Regional Bodies' (FSRBs) voice and participation in the FATF's work. This will ensure continued strengthening of and greater cohesion across the global network of over 200 jurisdictions to help achieve shared objectives and priorities of combatting illicit finance.

What this means:

Enhanced cohesion should support jurisdictions in sharing intelligence, aligning regulations, and responding more effectively to emerging threats, including cybercrime, virtual assets, and fraud.

8. Membership

The FATF suspension of the Russian Federation continues to stand (see February 2024 statement).

What this means:

Russia is excluded from participating in FATF decision-making and activities, reflecting ongoing concerns about its compliance with international AML/CFT/CPF standards. Other jurisdictions should remain cautious when dealing with Russian financial institutions, given the increased regulatory and reputational risks associated with cross-border transactions.



JMLSG Updates AML Guidance

In February, the Joint Money Laundering Steering Group (JMLSG) published amendments to key sections of its Part I guidance. The updates have now been submitted to HM Treasury for Ministerial approval.

Key changes

MLRO role and oversight (Chapter 3)

The updates provide greater clarity on the responsibilities and independence of the Money Laundering Reporting Officer (MLRO). They place increased emphasis on effective oversight of AML controls, robust governance arrangements, and clear internal reporting lines, alongside regular reviews of control effectiveness.

Data protection and SARs (Chapter 6)

The guidance has been updated on handling subject access requests where suspicious activity reports exist. The revisions align more closely with UK GDPR requirements and stress the need for careful, case-by-case assessment before any disclosure is made.

Who this affects:

- UK-regulated financial institutions subject to AML/CTF requirements
- MLROs and compliance teams
- Legal and data protection teams handling subject access requests in an AML context

What this means for firms:

Firms should review the updated guidance and ensure their AML frameworks reflect the strengthened expectations around MLRO responsibilities, governance, and oversight. Policies and procedures relating to SAR handling and data protection should be updated in line with the revised guidance, particularly in relation to subject access requests.

UK

HM Treasury Select Committee report on regulation of AI in financial services

The Treasury Select Committee has warned that the Bank of England, the Financial Conduct Authority (FCA), and HM Treasury's current approach to AI in financial services could expose consumers and the wider financial system to potentially serious harm.

While the report primarily focuses on consumer protection and financial stability, it also has clear implications for financial crime risk:

- **Operational and data risks:** AI in automated decision-making, credit scoring, transaction monitoring, and customer interactions can introduce vulnerabilities such as model bias, lack of explainability, or data integrity issues, which may be exploited or undermine controls.

- **Risk detection and controls:** Without clear regulatory expectations, firms may deploy AI in sensitive areas like fraud detection, sanctions screening, AML reporting, or transaction monitoring without adequate oversight, reducing effectiveness.

- **Third-party and model risk:** Reliance on external AI providers or systems increases the chance that processes fail to detect illicit activity, misclassify suspicious behaviour, or create systemic blind spots.

These points underline the need for robust governance, accountability, and validation of AI systems as part of AML/CFT and operational risk frameworks in an increasingly automated financial environment.

What this means for firms:

Firms need to ensure that AI tools are properly governed and validated, particularly when used for AML/CFT, fraud detection, sanctions screening, and transaction monitoring. They should maintain oversight over third-party AI providers, implement strong model risk management, and ensure auditability and explainability of automated processes. Failure to do so could result in blind spots in detecting financial crime, regulatory

Report Fraud launch:

On 20 February the City of London Police announced the full launch of Report Fraud, a new gateway for cyber crime and fraud reporting and intelligence. As announced in December 2025, Report Fraud replaces Action Fraud as the national reporting platform. The platform is designed to improve the collection, analysis, and dissemination of fraud intelligence, helping law enforcement and industry respond more effectively to evolving threats.

What this means for firms:

Firms should familiarise themselves with Report Fraud as the primary route for reporting incidents and suspicious activity. Integrating this platform into internal fraud reporting and escalation processes can improve timely notification to authorities, support intelligence sharing, and help firms identify emerging patterns of cyber-enabled fraud, enhancing AML/CFT and operational risk controls.

NCA launches the National Strategic Assessment 2026

The National Crime Agency (NCA) has published its 2026 National Strategic Assessment, highlighting that serious and organised crime in the UK is increasingly technology-driven, global, and interconnected. Criminal networks now exploit digital platforms, cryptocurrencies, AI, and sophisticated concealment methods to commit fraud, money laundering, drug trafficking, cybercrime, and human smuggling. The report emphasises the convergence of criminal markets, where financial crime is often embedded across multiple illegal activities.

The assessment stresses the need for intelligence-led, coordinated responses, stronger AML/CFT controls, transaction monitoring, and cross-sector collaboration to disrupt these networks. It also supports police reform proposals, including the creation of a National Police Service, to consolidate expertise and capabilities in tackling complex and transnational criminal threats.

What this means for firms:

Firms should recognise that financial crime risks are becoming more complex and interconnected.

Strengthening AML/CFT frameworks, monitoring for sophisticated and technology-enabled schemes, improving data analytics, and collaborating with law enforcement and industry partners are critical. Proactive engagement with emerging guidance and intelligence-sharing platforms will help firms mitigate risk and meet regulatory expectations in a rapidly evolving threat landscape.

Open call for evidence on economic crime information sharing

On 9 March, the Home Office launched a call for evidence on economic crime information sharing, seeking views on how data and information are shared to detect, prevent, investigate and disrupt economic crime across the UK. This initiative focuses on identifying legal, operational and cultural barriers that currently limit effective information sharing and on gathering ideas for reform to strengthen the overall framework.

The call invites responses from organisations and individuals across both the public and private sectors that play a role in tackling economic crime. It covers sharing of information relating to all forms of economic crime, including fraud, money laundering, corruption and asset recovery, reflecting the interconnected nature of these threats and their overlap with underlying offences to money laundering.

This call for evidence is part of broader efforts to enhance the UK's economic crime framework and prepare for future policy development aimed at improving data sharing systems and reducing the structural barriers that prevent timely, effective collaboration against serious financial crime.

What this means for firms:

Firms should anticipate potential reforms that could require more structured and timely sharing of information with regulators, law enforcement, and industry partners. Enhancing internal processes for reporting suspicious activity, improving collaboration with peers, and reviewing governance around data handling will be important to align with emerging expectations and reduce financial crime risk.

UK banks urged to stop blocking crypto firms to boost digital hub ambitions

The UK government, led by HM Treasury, has urged banks to stop restricting access to crypto firms, warning that doing so could undermine the UK's ambition to become a global digital asset hub.

Despite progress toward clearer crypto regulation, many banks continue to block or limit services to crypto businesses, even those authorised by the FCA. The government emphasised that regulated crypto firms should be treated fairly and not excluded simply due to their sector.

What this means for firms:

Crypto and financial services firms should expect continued government pressure on banks to provide fair access to banking services. Firms may benefit from clearer guidance on engaging with banks, but must maintain robust AML/CFT controls, regulatory compliance, and transparency to demonstrate they meet the standards expected by regulators and financial institutions.



OFSI consultation response on reform of the enforcement process:

On 9 February, HM Treasury's Office of Financial Sanctions Implementation (OFSI) published an updated Financial Sanctions Enforcement and Monetary Penalties Guidance, setting out how civil sanctions breaches will be assessed, enforced and penalised. Following a public consultation, OFSI intends to go ahead with proposals to do the following:

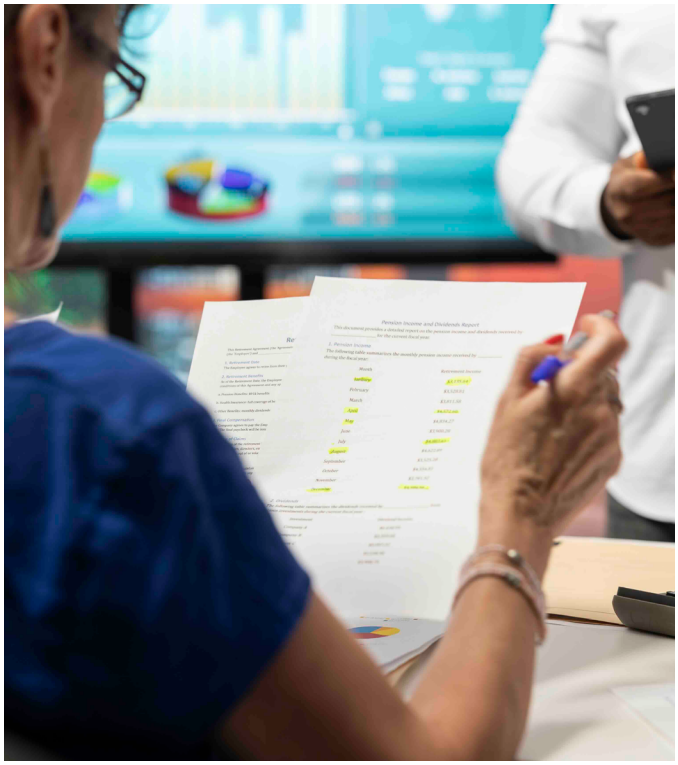
- Providing more guidance on how OFSI assesses cases, including revisions to the discounts applied.
- Reducing the maximum discount for voluntary

disclosure from 50% to 30%, and introducing two new discounts: an early account scheme discount (20%) and a settlement discount (20%) - for a new maximum discount of 70%. The settlement scheme means firms will be able to reach a settlement with OFSI, as opposed to waiting for a penalty, by waiving their right to appeal.

- The early account scheme will be introduced to expedite cases, which will allow firms to submit a full and comprehensive early account of the breach, which may in practice involve commissioning third-party investigations, although OFSI does not mandate this.
- Greater clarity around enforcement of information, reporting or licensing offenses (where no funds have been made available, but the institution fails on their reporting requirements). Increased maximum penalty amount from £1 million to £2 million of 100% of the value of the breach.

What this means for firms:

While potential penalties are higher, firms now have stronger incentives to settle early and engage proactively, including commissioning independent investigations to demonstrate compliance. The changes encourage transparency, speed up OFSI enforcement processes, and highlight the importance of robust sanctions compliance frameworks and reporting procedures.



APP scams reimbursement dashboard for Q3 2025

The Payment Services Regulator (PSR) has published performance figures for the first 12 months of mandatory reimbursement of authorised push payment (APP) fraud.

The dashboard shows that the UK's new APP scam reimbursement rules (introduced October 2024) are having a positive impact on consumers.

In the first year (between 7 October 2024 to 30 September 2025):

- 88% (£173m) of the money lost to APP scams has been reimbursed to victims. For comparison, UK Finance reported a 65% reimbursement rate in 2024.
- Consumers have reported around 269,000 claims; 188,000 were in scope for reimbursement. This is around 15% fewer claims than the previous year.
- 82% of claims were closed within five business days – and 98% within 35 business days.
- 3% of claims rejected due to the customer not taking enough care over the transaction or their claim.

What this means for firms:

Firms need to maintain robust fraud detection, reimbursement processes, and timely claims handling to comply with the rules and minimise reputational and regulatory risk. Early reimbursements and effective transaction monitoring are crucial to meeting PSR expectations and protecting consumers against APP scams.

The role of the FCA and PSR in delivering the National Payments Vision

On 2 February,the FCA and the PSR outlined their role in delivering the UK's National Payments Vision through a speech at the Payments Regulation and Innovation Summit:

Strong and longstanding collaboration across the Payment Authorities has been key to the impressive changes delivered to date on payments systems.

The National Payments Vision is an opportunity to deliver a world-leading payments sector that drives growth and innovation, while serving users, facilitating competition, and ensuring security.

What this means for firms:
Firms should expect continued regulatory focus on operational resilience, security, and consumer protection as the payments ecosystem evolves. This includes adapting to new infrastructure, ensuring robust controls, and maintaining compliance with PSR and FCA guidance. Forward-looking firms can leverage these developments to enhance services, adopt innovative payment solutions, and strengthen fraud and financial crime controls in line with the National Payments Vision.

Payments Forward Plan

The Payments Forward Plan sets out a coordinated regulatory roadmap to deliver the UK's National Payments Vision over the next three years. The Plan outlines how HM Treasury, the Bank of England, the FCA, and the PSR will modernise payment regulations, upgrade critical payment infrastructures, and support innovation across the retail and wholesale payments ecosystem. It includes forthcoming work on payment services legislation, digital assets (including stablecoins), Open Banking and Open Finance, and the design of the Digital Pound. It also provides sequencing to avoid regulatory congestion and ensure that changes are manageable for firms.

What this means for firms:
Firms should prepare for substantial regulatory and infrastructural change, including updates to payments law, new technical standards, modernised payment rails, and new frameworks for stablecoins and Open Finance. They should also ensure operational resilience, monitor future consultations closely, and position themselves to take advantage of innovation opportunities enabled by the modernisation of the UK's payments ecosystem.



First firms join FCA's Scale-Up Unit

On 3 February, the Bank of England and the FCA announced the first cohort of banks and building societies to join their joint Scale-Up Unit, a new initiative aimed at supporting fast-growing banks and building societies as they expand, innovate and navigate complex regulatory requirements

The Scale-Up Unit, announced last year, is designed to build stronger ties and provide tailored support for fast-growing and innovative financial firms, helping them to grow sustainably at pace.

The first cohort consists of: Allica; ClearBank; Monument; Nottingham Building Society; OakNorth; Zopa.

While the announcement focuses on growth and innovation, regulators' engagement with these firms may also cover areas such as governance, risk management, and operational resilience, which underpin compliance with financial crime and regulatory obligations.

What this means for firms:
For the selected firms, joining the Scale-Up Unit means closer engagement with the PRA and FCA as they grow, giving them tailored support while ensuring they strengthen governance, risk management and operational resilience as they scale. For the wider sector, it signals that regulators expect fast-growing firms to invest early in robust controls and to be prepared for more proactive supervisory attention as they expand.

Single UK Sanctions list

The UK government's sanctions lists changed to a single list on 28 January. UK sanctions designations are now only detailed in the UK Sanctions List (UKSL), published by the Foreign, Commonwealth and Development Office.

The Consolidated List of Asset Freeze Targets, which was published for HM Treasury by OFSI, is no longer being updated. It is available for reference purposes on its old page.

What this means for firms:
Firms must now rely solely on the UKSL for all sanctions checks and update their internal screening

systems accordingly. Using outdated lists could result in compliance gaps, so firms should review and revise policies, procedures, and automated systems to ensure accurate, up-to-date sanctions screening, reporting obligations, and risk management.

Ownership and Control Test in UK Financial Sanctions Regulations

On 16 February, HM Treasury launched a call for evidence to seek industry's views on how UK financial sanctions regulations on ownership and control are applied in practice, including how firms implement the regulations and where they face challenges. This call for evidence closes on 13 April 2026.

What this means for firms:

Firms should track this review closely, as HM Treasury may refine the ownership and control rules or publish additional guidance. The call for evidence highlights regulators' recognition that firms face practical challenges in assessing complex ownership structures and "hypothetical control", meaning firms should ensure their sanctions frameworks, particularly governance, escalation processes, and due diligence methodologies are robust, well-documented, and aligned with current obligations. Strengthening these controls now will help firms adapt efficiently to any future regulatory changes.

FCA's Regulatory Priorities reports

The FCA is introducing nine annual Regulatory Priorities reports to replace its portfolio letters. The reports will provide specific key priorities for each sector and are meant to provide a clearer, more consistent way of communicating what the FCA expects and where to focus.

These reports provide:

- Specific key priorities for each sector.
- Further relevant work the FCA will be undertaking in the next year.

What this means for firms:

Firms should review the report relevant to their sector to understand the FCA's expectations, ensure their compliance programs align with identified priorities, and focus resources on the areas of greatest supervisory interest. This provides an opportunity to proactively address emerging risks, regulatory gaps, and industry-wide issues before they become enforcement concerns.

Using digital identities with the Money Laundering Regulations

The UK Government has published guidance on how the UK Digital Identity and Attributes Trust Framework and the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) interact. It is approved guidance for the purposes of compliance with the MLRs. It begins with an overview of digital identities and the Framework, and then explores the intersection of the framework with the MLRs to help organisations understand how they can use digital identities to fulfill some of their obligations under the MLRs.

What this means for firms:

Firms can consider adopting digital identity solutions to streamline identity verification and reduce reliance on physical documentation, while still meeting MLR obligations. This can improve efficiency, reduce fraud risk, and strengthen compliance, provided that the digital identities used meet the trust framework standards and are applied consistently within AML/CFT controls.

Supervision of Payment Services and Electronic Money

The FCA has published finalised guidance clarifying its supervisory approach to payment services and e-money firms. The guidance reinforces expectations around safeguarding, governance, and wind-down planning, with a clear focus on consumer protection and operational resilience.Enhanced expectations for safeguarding of client funds and reconciliation processes

- Enhanced expectations for safeguarding of client funds and reconciliation processes
- Greater emphasis on governance and senior management accountability
- Requirement for robust wind-down planning
- Clarification that firms remain responsible when using outsourcing and third parties

The Approach Document will be further updated when the Supplementary Regime goes live on 7 May 2026, introducing additional regulatory expectations for firms.

The guidance reflects a more proactive supervisory stance, requiring firms to demonstrate stronger controls, governance, and protection of customer funds.

What this means for firms:
Firms should expect closer FCA scrutiny of safeguarding arrangements, governance, outsourcing oversight, and wind-down planning, and ensure these areas are fully documented and robust. The updated Approach Document signals a more proactive supervisory stance, meaning payment and e-money firms must strengthen operational resilience, keep customer funds protected, and prepare for additional expectations coming with the May 2026 Supplementary Regime. Those offering contactless payments must also ensure SCA exemptions and limits are applied in line with the March 2026 updates.

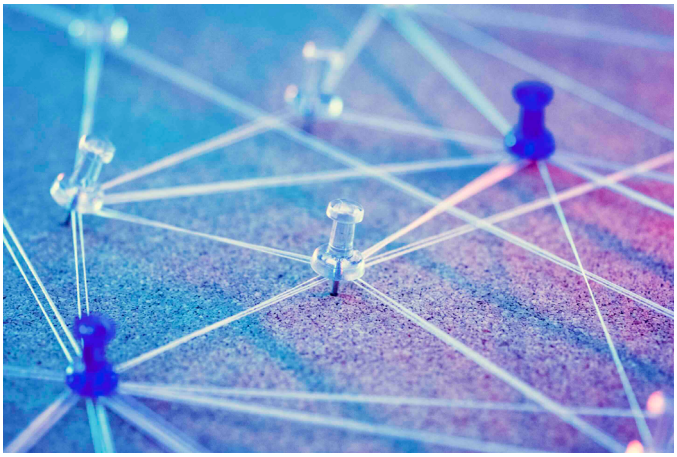
Statutory guidance on the meaning of "significant influence or control"

The UK Government has updated statutory guidance on identifying individuals with significant influence or control (PSC) over companies, providing further clarity on ownership and control structures. The guidance:

- Clarifies what constitutes "significant influence or control", beyond shareholding thresholds
- Emphasises identification of individuals who can direct or influence company decisions, formally or informally
- Highlights risks of complex or opaque ownership structures, including nominee or indirect arrangements
- Reinforces the need for firms to take a substance-over-form approach when identifying beneficial owners

The updated guidance strengthens expectations on firms to look beyond formal ownership and ensure accurate identification of ultimate controllers, supporting transparency and effective AML controls.

What this means for firms:
Firms will need to apply a more rigorous, substance-over-form approach when identifying people with significant control, looking beyond formal ownership and assessing both rights-based and behaviour-based influence. This means strengthening beneficial ownership checks, documenting PSC assessments more thoroughly, and reviewing complex or opaque structures, particularly where indirect influence, nominee arrangements, or informal control may exist. The updated guidance raises expectations for transparency and supports stronger AML and corporate governance controls.





UK National Fraud Strategy

Fraud remains the most common crime in the UK, causing significant harm to individuals, businesses and the wider economy. As fraud becomes increasingly sophisticated and digitally enabled, it continues to erode public trust and is now closely linked to organised crime.

In response, the UK Government's updated Fraud Strategy (March 2026) sets out a strengthened approach focused on preventing fraud at source, improving coordination across government, industry and law enforcement, and increasing the disruption of criminal networks.

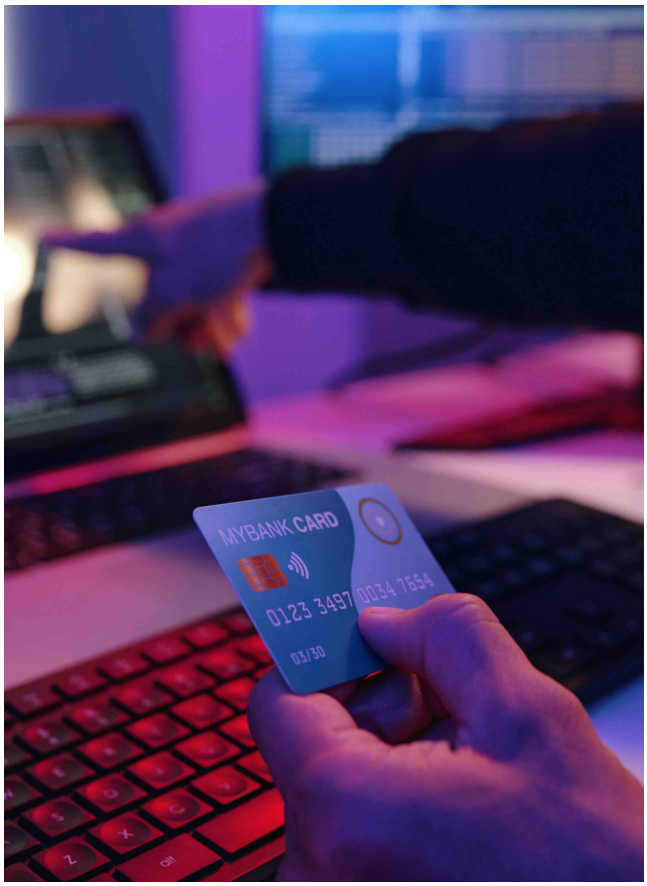
The strategy is built around three pillars — Pursue, Prevent and Protect — with a clear emphasis on stopping fraud before it occurs and better supporting victims. A central theme is the need for closer public-private collaboration, particularly with banks, telecoms providers and technology platforms, recognising that fraud prevention requires a coordinated, ecosystem-wide response.

There is also a notable shift towards placing greater responsibility on firms whose services are exploited by fraudsters. Online platforms and telecoms providers are expected to do more to tackle scam content, spoofing and phishing activity, while payment service providers are under increasing pressure to strengthen fraud detection and improve reimbursement outcomes for victims of APP scams.

Alongside this, the strategy highlights the importance of enhanced data sharing and intelligence use to identify fraud networks earlier, as well as continued investment in law enforcement capabilities. Consumer awareness also remains a key priority, supported by campaigns to help individuals recognise and avoid scams. The growing role of technology, particularly AI, is recognised as both a driver of fraud risk and a critical tool in improving detection and prevention.

What this means for firms:

Firms across financial services, telecoms and technology sectors should expect increased scrutiny of their fraud controls, particularly in digital channels. Strengthening transaction monitoring, customer protection measures and intelligence-sharing arrangements will be key, alongside demonstrating clear governance over fraud risks, especially in relation to APP scams and cross-border, tech-enabled threats.



UK Money Laundering and Terrorist Financing (Amendment) Regulations 2026

The UK Government has introduced the Money Laundering and Terrorist Financing (Amendment) Regulations 2026, updating the existing AML/CTF framework to strengthen controls and address emerging risks.

- Pooled account risk: Firms providing pooled client accounts must understand their use and associated ML/TF risks and take appropriate mitigation steps.
- Crypto and correspondent relationships: Enhanced due diligence requirements are introduced for cryptoasset exchange providers, custodial wallet providers, and certain correspondent banking relationships.
- Due diligence updates: Clarifies when enhanced due diligence is required, including for unusually complex or large transactions, and aligns thresholds with sterling.
- Trust register reforms: Refinements to trust registration requirements improve transparency of beneficial ownership.
- Supervisory enhancements: Firms must notify the regulator of material changes or inaccuracies in AML/CTF information, strengthening oversight and reporting.



Implementation:
Most changes take effect shortly after enactment, with certain provisions (e.g. crypto) phased in over time, including a key compliance date of 1 February 2027 for specific requirements.

The 2026 Regulations reinforce the UK's commitment to modernising AML/CTF controls, particularly for crypto, pooled accounts, and high-risk relationships, and require firms to update policies, systems, and risk assessments accordingly.

What this means for firms:
Firms will need to update their AML/CTF frameworks to reflect strengthened requirements, particularly around pooled accounts, cryptoasset due diligence, and enhanced risk assessment thresholds. Policies, systems, and customer due-diligence processes must be revised, and firms should plan for phased implementation timelines.



Launching Digital Identity: Introducing the 1.0 Trust Framework

In March 2026, the UK government introduced version 1.0 of its Digital Verification Services (DVS) trust framework, intended to shape a more reliable digital identity ecosystem. The framework sets out the core rules and standards that providers must meet, giving firms and users greater confidence in the security and consistency of certified services. Supporting guidance and supplementary codes provide more detailed direction for specific use cases and sectors, helping the framework adapt to different parts of the market while maintaining a common baseline for trust.

What this means for firms:

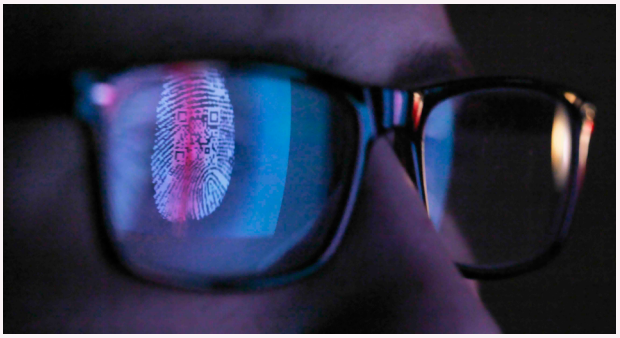
The launch of the framework gives firms a clear, government-approved standard for using certified digital identity services with confidence. Businesses can now adopt verified digital identity solutions knowing they meet defined security and assurance requirements, enabling faster onboarding, reduced fraud risk, and more consistent identity verification. Firms operating in regulated sectors should prepare to align their digital ID processes with the trust framework and any supplementary codes relevant to their industry.

Consultation on National Digital ID

The UK government has launched a consultation on proposals for a national digital identity system, open until 5 May. The initiative would cover British and Irish citizens, as well as foreign nationals with permission to be in the UK, and is intended to sit at the centre of future digital public services.

The proposal aims to make interacting with government services as easy as the public's experience with the private sector, such as online banking. It also sets out plans for a strengthened trust framework for digital identity providers, clearer verification standards, and improved interoperability between public and private sector systems.

A key objective is to enable individuals to verify their identity once and reuse it securely across multiple services, reducing friction and duplication.





UK Government's strategic approach to sanctions enforcement

The UK Government has published a cross-government strategy on sanctions enforcement to improve industry understanding of enforcement expectations, strengthen compliance, and increase the deterrent effect of UK sanctions. The document consolidates roles and responsibilities across government bodies, including the civil and criminal enforcement tools available for sanctions breaches, and highlights the importance of robust compliance systems, voluntary disclosure and cooperation in enforcement outcomes.

Sanctions enforcement: Responsibilities at a glance

Type of Sanction	Civil Responsibility	Criminal Responsibility
Financial	Office of Financial Sanctions Implementation	National Crime Agency
Oil Price Cap	Office of Financial Sanctions Implementation	HM Revenue and Customs National Crime Agency
Trade	Office of Trade Sanctions Implementation	HM Revenue and Customs
Transport	Department for Transport	National Crime Agency
Internet Services	The Office of Communications (OFCOM)	HM Revenue and Customs
Immigration	Home Office	Home Office
Director Disqualification	Insolvency Service	Insolvency Service

Europe

European Commission updated high-risk third country list

The European Commission updated its high-risk third country list, effective 29 January, identifying jurisdictions with strategic deficiencies in their AML/CFT frameworks. Firms are required to apply enhanced due diligence when dealing with higher-risk jurisdictions. The list supports a more consistent, risk-based approach across Member States and helps mitigate exposure to financial crime linked to cross-border activity.

What this means for firms:

Firms should review and update country risk assessments, screening systems, and customer due diligence processes to ensure enhanced controls are applied where required.

EBA and AMLA complete handover of AML/CFT mandates

As of January, the EU's new Anti-Money Laundering Authority (AMLA) has assumed AML/CFT supervisory responsibilities for certain financial institutions from the European Banking Authority (EBA). This is part of AMLA's central role in leading, coordinating and shaping AML supervision across the EU, part of a broader reform to strengthen the region's financial crime framework.

AMLA is designed to ensure a more harmonised and integrated supervisory system, with a mandate to promote consistency across Member States, oversee higher-risk institutions, and support the development of a single EU AML rulebook.

What this means for firms:

Firms should expect more consistent supervisory expectations and increased scrutiny across the EU, particularly in higher-risk areas, as AMLA drives greater convergence in AML/CFT standards.

AMLA consults on harmonised AML/CFT standards for the private sector

AMLA has launched consultations on key mandates aimed at developing harmonised standards for customer due diligence across both financial and non-financial sectors in the EU. These consultations cover draft Regulatory Technical Standards (RTS) designed to promote consistent application and enforcement of AML/CFT requirements across Member States.

What this means for firms:

Firms should contribute to these consultations where appropriate, and monitor the outcomes as they are likely to lead to more standardised and prescriptive AML/CFT requirements across the EU, particularly in relation to customer due diligence and supervisory expectations.

MONEYVAL report on virtual assets and financial crime risks

In February, the Council of Europe's anti-money laundering body MONEYVAL published an updated report examining the use of virtual assets and virtual asset service providers (VASPs) in money laundering, terrorist financing, and sanctions evasion. The report provides a cross-jurisdictional review based on input from 25 member states, highlighting how rapid developments in crypto technology are creating new financial crime risks.

It identifies vulnerabilities in the regulation and supervision of the VASP sector, with particular focus on the use of virtual assets to circumvent targeted financial sanctions and facilitate illicit financial flows.

What this means for firms:

Firms should strengthen controls around crypto-related activity, including enhanced due diligence, transaction monitoring, and sanctions screening, particularly where there is exposure to cross-border or higher-risk virtual asset activity.

EU strengthens terrorist sanctions framework

The Council of the European Union has updated its counter-terrorism sanctions regime, strengthening the scope of the EU terrorist list while maintaining all existing designations.

The changes are aimed at ensuring the framework remains flexible and effective in addressing evolving terrorist threats. The revised approach enhances the EU's ability to target individuals and entities involved in supporting, facilitating, or financing terrorism, while reinforcing the legal and operational foundations for future designations.

What this means for firms:

This development is a reminder of the importance of maintaining robust and up-to-date sanctions screening controls, particularly in managing terrorist financing risks and cross-border exposure.

Highlights from around the world

United States: Treasury Publishes 2026 National Risk Assessments

The US Department of the Treasury has released its latest suite of National Risk Assessments, covering terrorist financing, money laundering and proliferation financing. Together, the reports provide a view of evolving illicit finance risks, with a strong emphasis on the growing role of digital channels, complex networks and cross-border activity.

National Terrorist Financing Risk Assessment

The updated terrorist financing assessment finds that overall risk levels remain relatively low, but threats are becoming more decentralised, digital and harder to detect.

- **Al-Qaeda affiliates** continue to rely on local revenue streams such as extortion, taxation and natural resource exploitation, with groups like Al-Shabaab demonstrating strong financial capability.
- **ISIS affiliates** have shifted towards smaller-scale, decentralised funding, including extortion, kidnapping, looting and online donations.
- **Hamas** draws on a mix of state support, charities, diaspora funding and commercial activity, often facilitated through regional networks.
- **Hezbollah** combines state funding with income from both legitimate businesses and illicit activities such as smuggling and organised crime.
- **Domestic violent extremists (DVEs)** are typically self-funded, increasingly using online platforms, making detection more challenging.

Overall, the report highlights a trend towards more fragmented and digitally enabled financing models, reinforcing the need for strong risk-based controls and cross-channel monitoring.

National Money Laundering Risk Assessment

This assessment draws on government data, law enforcement casework, anti-money laundering reporting intelligence, and international developments to support both public- and private-sector efforts to understand and combat money laundering. It will also feed into the 2026 National Illicit Finance Strategy.

- **Key predicate offences** continue to include fraud, drug trafficking, cybercrime, human trafficking and corruption.
- **Professional laundering networks**, including organised groups and money mule schemes, play a significant role in obscuring illicit funds.

- **Technology and digital channels** such as encrypted communications, social media and digital assets — are increasingly used to move value quickly across borders.
- **System-wide exploitation** remains prevalent, with criminals leveraging a range of channels, from traditional banking and cash to digital assets and legal entities.

The assessment underscores the need for firms to incorporate these evolving risks into their AML frameworks, particularly the intersection of traditional crime with digital and network-enabled laundering techniques.

National Proliferation Financing Risk Assessment

The proliferation financing assessment focuses on how financial systems are exploited to support the development and movement of weapons of mass destruction.

- **State-linked threats** remain most significant, particularly from North Korea and Iran, with Russia also posing notable risks through efforts to acquire dual-use goods.
- **Sanctions evasion networks** including actors in China and other jurisdictions play an increasing role in facilitating prohibited activity.
- **Structural vulnerabilities** in the financial system, including the global role of the U.S. dollar and gaps in controls (notably in digital asset sectors), continue to be exploited.
- **Key typologies** include the use of digital ecosystems to raise and move funds, alongside more traditional methods such as front companies, intermediaries and trade-based evasion.

The report highlights the close links between proliferation financing, sanctions evasion and broader AML/CFT risks, reinforcing the need for integrated controls and enhanced monitoring.

What this means for firms:

Across all three assessments, a consistent theme is the increasing complexity, digitalisation and interconnectedness of illicit finance risks. Firms should ensure their risk assessments, monitoring capabilities and controls are evolving accordingly, with a particular focus on technology-enabled threats, networked activity and cross-border exposure.

Guidance on sham transactions and sanctions evasion

In March 2026, OFAC released a sanctions advisory warning that sanctioned individuals increasingly use sham transactions, such as transfers through proxies, opaque structures, or family members to disguise their continuing property interests. The advisory provides indicators to help firms identify when property may still be controlled by a blocked person despite purported divestment.

FinCEN Advisory on Health Care Fraud Schemes Targeting Medicare, Medicaid, and Other Federal and State Health Care Benefit Programs

In March, FinCEN published an Advisory on Health Care Fraud Schemes Targeting Medicare, Medicaid, and Other Federal and State Health Care Benefit Programs to urge financial institutions to be vigilant in identifying and reporting suspicious transactions potentially related to health care fraud schemes targeting Medicare, Medicaid, and other Federal and state health care benefit programs). The advisory highlights the use of straw owners and shell companies to register as Health Care Providers and suppliers and obfuscation of fraudulent reimbursements through the U.S. and international financial systems.

Key enforcement actions: Lessons learned

Enforcement Watch
The FCA published an Enforcement Watch 1 newsletter in January, which is the inaugural edition of a new publication designed to give regulated firms insight into the FCA's enforcement activity, priorities and approach following its updated Enforcement Guide.

Key points:

- Publicity policy: The FCA can signal investigations earlier, naming firms/ individuals only in "exceptional circumstances" (e.g. consumer protection).
- Enforcement priorities (Jun–Dec 2025): 23 new cases covering financial crime, individual misconduct, unauthorised business (crypto), market disclosure, consumer duty breaches, weak controls, and oversight failures.
- International cooperation: The FCA works with global regulators and law enforcement to support cross-border investigations.

Who's impacted: Regulated firms, listed issuers, senior managers, compliance/ AML teams, crypto and consumer-focused firms.

UK
Sanctions violation by Apple Distribution International (ADI)
OFSI has fined Apple Distribution International (ADI) £390,000 for breaching the UK's Russia sanctions by making payments to a sanctioned entity via a UK bank. Payments were voluntarily disclosed, resulting in a reduced penalty. National fraud he breach was in scope of UK regulations despite ADI being an Irish entity; a UK nexus was applied due to the use of a UK financial institution.

Key takeaways:

- Sanctions scope extends beyond UK firms: UK sanctions can apply wherever UK financial infrastructure is involved - including clearing, correspondent banking or payments routed through the UK - regardless of where a firm is headquartered.
- Ongoing monitoring is essential: Sanctions risk is not static. Firms need to track changes in counterparty ownership and control, and ensure screening processes are robust, up to date and capable of identifying indirect exposures.
- Cooperation can mitigate enforcement outcomes: Voluntary disclosure of breaches, alongside proactive engagement with regulators, can lead to reduced penalties and more favourable outcomes.
- Accountability sits with the firm executing the transaction: Responsibility for sanctions compliance cannot be outsourced. Even where third parties are involved, the paying or transacting entity retains ultimate accountability.



OFSI fines Bank of Scotland for Russia sanctions breaches

OFSI has fined Bank of Scotland £160,000 for breaches of the UK's Russia sanctions regime. The failings stemmed from weaknesses in sanctions screening and escalation processes, including poor handling of name variations, lack of enhanced screening tools, and human error during customer review. As a result, a sanctioned individual was able to access and move funds for over two weeks. While the case was deemed serious, the penalty was reduced by 50% due to voluntary disclosure.

Key takeaways:

- **Screening must capture real-world complexity:** Systems need to be capable of identifying name variations and indirect matches.
- **Enhanced screening is expected in higher-risk contexts:** Reliance on standard lists alone may be insufficient; firms should consider additional data sources and controls where sanctions risk is elevated.
- **Human oversight remains a key vulnerability:** Errors in manual review processes (e.g. PEP or sanctions assessments) can undermine otherwise robust systems, highlighting the need for strong controls, training and quality assurance.
- **Control failures can quickly lead to breaches:** Even short delays in identifying and restricting sanctioned individuals can result in prohibited transactions and regulatory action.
- **Voluntary disclosure can materially reduce penalties:** Proactive engagement with regulators can significantly mitigate financial consequences, even in serious cases.

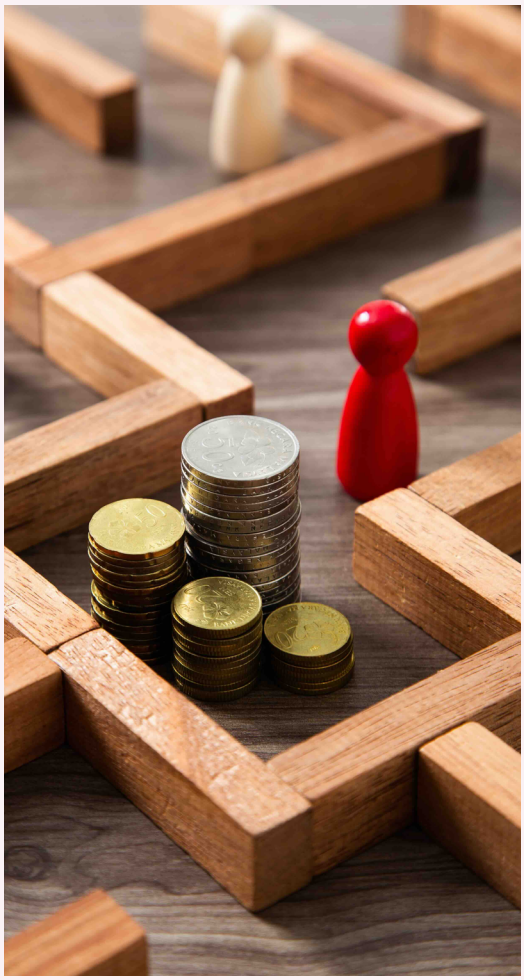
FCA imposes restrictions on Sendsii Ltd

The FCA has issued a First Supervisory Notice to Sendsii Ltd after HM Revenue and Customs (HMRC) suspended the firm's registration on 9 October 2025. The suspension means that Sendsii Ltd no longer met the conditions required for its FCA authorisation under the Payment Services Regulations 2017.

In January, the FCA imposed requirements on Sendsii Ltd which prevent Sendsii from carrying out any regulated activity, including money remittance, without the FCA's prior written consent. The firm is required to return all funds held for or on behalf of existing customers in accordance with all relevant legal and regulatory requirements.

Key takeaways:

- **Regulatory permissions can be lost quickly:** A suspension by another authority (e.g. HMRC) can directly impact FCA authorisation. Firms must ensure ongoing compliance across all relevant regulators.
- **Business disruption risk is immediate:** Restrictions can halt all regulated activity, including core services like money remittance, with little notice.
- **Safeguarding obligations remain critical:** Even under restriction, firms must return customer funds promptly and in line with regulatory requirements.
- **Third-party dependencies matter:** Issues with registrations (e.g. under MLRs) can have wider knock-on effects across permissions and operations.



US

FTC moves to hold payment processors in contempt

On 13 January, the US Federal Trade Commission (FTC) asked a federal court to hold several payment processors in contempt for allegedly breaching a 2015 order. The FTC claims the firms continued to process payments for high-risk merchants including those flagged for fraud, while failing to implement adequate monitoring and controls. The action, which seeks $52.9m in penalties, signals a more aggressive use of enforcement powers to address ongoing non-compliance and protect consumers.

Key takeaways:

- **Regulators expect strict adherence to legacy orders:** Historic enforcement actions are not "one and done"; firms must continue to comply fully over time.
- **High-risk merchant monitoring is critical:** Payment processors are expected to actively identify, monitor and, where necessary, offboard high-risk or fraudulent clients, not simply rely on initial onboarding checks.
- **Failure to act on red flags increases exposure:** Processing transactions for merchants on fraud watchlists or with known risk indicators can be viewed as systemic control failure, not isolated oversight.
- **Enforcement is becoming more punitive and public:** The use of contempt proceedings - alongside significant financial penalties - highlights a willingness to escalate enforcement for repeated or deliberate breaches.

Bank of Ireland UK: Failure to comply with Confirmation of Payee

On 5 March 2026, the PSRr fined Bank of Ireland UK £3,779,300 for failing to comply with Confirmation of Payee (CoP) requirements, identifying deficiencies in the implementation and operation of the service. The PSR found that weaknesses in name-checking controls increased customers" exposure to APP fraud. The case reinforces that firms must ensure CoP is not only implemented but operates effectively and consistently in practice, with appropriate oversight and controls.



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.