

REGCAP

SEPTEMBER 2026

A summary of the latest FinCrime
regulatory news

GLOBAL.



FATF finds hawala and underground banking remain key channels for professional money laundering networks

On 3 September 2026, FATF published a [report](#) on underground banking and hawala, concluding that informal value transfer systems remain a core channel used by professional money laundering networks to move illicit proceeds internationally. The report describes these networks as increasingly operating in combination with digital payment rails and cryptocurrency, blending traditional hawala settlement with online and crypto-based transfer methods rather than existing as a purely offline, cash-based system. FATF notes that this hybrid model can be difficult to detect using conventional transaction monitoring. Each stage of a transfer may look routine on its own, and the risk only becomes apparent when the stages are viewed together.

WHAT THIS MEANS FOR FIRMS

Firms with exposure to remittance corridors, money service businesses, or correspondent relationships serving diaspora or trade-finance communities should consider whether their typology library and transaction monitoring scenarios account for hybrid informal value transfer patterns (for example, mismatched counterparty-to-purpose narratives, or clusters of small transfers to the same beneficiary network from unrelated payers), rather than relying solely on rules built around pure cash-based hawala.



FATF report on the risks of gaming and gambling

On 9 September 2026, FATF published a [report](#) on the risks of gaming and gambling, warning that criminals are increasingly exploiting these sectors to launder money, including through non-gambling activity, “smurfing”, suspicious or coordinated bets, and illegal gambling markets. Illegal gambling is identified as one of the sector’s most significant risks, with illegal markets in some jurisdictions rivaling or exceeding legal gambling markets, and offshore operators often disguising themselves as legitimate businesses while offering anonymity and incentives attractive to criminals. FATF has published new risk indicators for governments, regulators and businesses, drawing on research and input from more than 80 jurisdictions and industry experts across casinos, gambling and video gaming.

FATF report on the risks of gaming and gambling (continued)

WHAT THIS MEANS FOR FIRMS

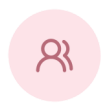
Firms should reassess their risk exposure, particularly where they have customers, transactions, payment flows or counterparties connected to gambling, gaming, online platforms or offshore operators. Transaction monitoring controls should be reviewed against the FATF indicators, such as multiple accounts or payment methods, transactions inconsistent with the customer's profile, rapid movement of funds with little/no gambling activity, unusual betting patterns and links to potentially illegal or unlicensed operators.

**FATF publishes Mutual Evaluation Reports for Canada and Turkey**

In September 2026, the Financial Action Task Force (FATF) published 5th round Mutual Evaluation reports for [Canada](#) and [Turkey](#), evaluating system effectiveness against the 11 Immediate Outcomes. Both countries strengthened their anti-illicit finance defences, with Canada advancing beneficial ownership transparency, and Turkey enhancing financial intelligence use and international cooperation. Both countries received 3 year roadmaps of Key Recommended Actions, with Turkey placed under enhanced follow-up and Canada under regular follow-up.

WHAT THIS MEANS FOR FIRMS

No immediate action.

**New Egmont Group report on the role of FIUs in the preparation of strategic intelligence**

The Egmont Group has published a [report](#) examining how financial intelligence units (FIUs) use strategic intelligence to identify money laundering and terrorist financing risks, support national risk assessments, and inform policy and operational decisions. It finds that while many FIUs have established strategic intelligence functions, there is scope to improve data access, analytical capabilities, institutionalisation, and the impact of intelligence on decision-making. The report highlights how transforming strategic intelligence into actionable insights can support FIUs with taking risk-based approaches to combating financial crime.

WHAT THIS MEANS FOR FIRMS

No immediate action.

UK.

FCA finds money mule activity shifting toward e-money institutions and challenger banks

On 23 September 2026, the Financial Conduct Authority (FCA) published [findings](#) from a multi-firm review into money mule activity, drawing on data from 35 firms including retail banks, building societies, challenger banks, payment institutions and e-money institutions. The review found that firms closed 238,396 suspected mule accounts in 2025. While retail banks process the highest transaction volumes through mule accounts, the FCA found that e-money institutions and payment institutions see a different pattern: fewer transactions, but at higher individual value, and a materially faster account lifecycle, with the review highlighting that criminals typically layer funds through several accounts before cashing out, most often between the second and fifth transfer.



WHAT THIS MEANS FOR FIRMS

Firms should look specifically at how quickly a new account needs to show a pattern before it is reviewed, given the review's finding that mule activity is often concentrated in the second-to-fifth transfer rather than emerging only after sustained use. Firms should also consider whether monitoring thresholds are tuned for lower-volume, higher-value payment flows (the pattern the FCA found most common outside retail banking) and are effective at catching layering activity.

HM Government publishes AML and Asset Recovery Strategy 2026 to 2029

On 15 September 2026, the UK Government published its [Anti-Money Laundering and Asset Recovery Strategy 2026-2029](#), setting three objectives (more effective and efficient defences; disrupting high-harm criminal networks; recovering more criminal assets) delivered through three pillars (target, integrate, empower), backed by £520m from the Economic Crime Levy over three years. The strategy does not itself create new obligations for firms.

HM Government publishes AML and Asset Recovery Strategy 2026 to 2029 (continued)

WHAT THIS MEANS FOR FIRMS

This signals the key government priorities over the strategy period. The emphasis is on reducing box-ticking in favour of harm-focused prioritisation, as well as better information-sharing between agencies and firms. While there is no immediate action for firms, FIs may wish to consult the Strategy when reviewing their internal financial crime risk assessment methodology.

FCA opens enforcement investigation into Euro Exchange Securities UK Ltd

On 17 September 2026, the FCA confirmed it has opened an [investigation](#) into Euro Exchange Securities UK Ltd (EES), an e-money and payment services firm, for potential breaches of the Money Laundering Regulations 2017, specifically around risk assessment, customer due diligence (CDD), ongoing monitoring and internal governance. The investigation covers the period from February 2020 to June 2026. EES had already been required to cease regulated e-money and payment activities on 4 June 2026, with the High Court appointing special administrators shortly after, and a First Supervisory Notice confirming the firm could not resume services published on 2 August 2026.

**WHAT THIS MEANS FOR FIRMS**

The FCA's decision to keep investigating a firm that had already left the market, rather than closing the file once the immediate harm was contained, shows the failings were serious enough to justify a historical look-back. The underlying issue, however, is whether controls were robust over time. Firms should first check that their CDD, ongoing monitoring and governance controls are fit for purpose. They should then consider whether those controls have worked consistently, and are evidenced well enough, to withstand a retrospective review covering several years.

Revolut confirms customer data breach via impersonation of a government agency

According to media reports, Revolut has [confirmed](#) that a third party had impersonated a government agency, using a lookalike or compromised official domain email to submit fraudulent requests for customer information. Revolut has said a limited number of customers were affected, with exposed data potentially including identity documents, contact details, and account or transaction information. Revolut stated its systems and customer funds were not affected, that it has blocked the fraudulent sender, and that it has notified affected customers, law enforcement and relevant regulators. Additional customers in Ireland were also confirmed to have been affected later in September.



WHAT THIS MEANS FOR FIRMS

This highlights that fraud risk also affects compliance and customer service teams handling seemingly official requests, not only customer payments. Firms should check how requests claiming to come from law enforcement, courts, or government bodies are verified before any customer data is disclosed: specifically, whether verification relies on anything the requester controls (a reply-to address, a phone number given in the request itself) rather than an independently sourced contact route, and whether there is a four-eyes check before sensitive data leaves the firm.

First prosecutions under ECCTA for directors failing to complete identity verification

On 17 September 2026, the Insolvency Service [announced](#) the first prosecutions for breaches of the director identity verification requirements under the Economic Crime and Corporate Transparency Act (ECCTA) 2023. Three directors were fined for failing to verify their identity with Companies House. From 18 November 2025, newly appointed directors have had to verify their identity before acting, with existing directors given a 12-month transition window tied to their confirmation statement filing. Companies House's Director of Intelligence and Law Enforcement Engagement, Martin Swain, called the prosecutions "an important milestone in strengthening the integrity of the UK's company register".

First prosecutions under ECCTA for directors failing to complete identity verification (continued)

WHAT THIS MEANS FOR FIRMS

The fines themselves are modest, but this signals that ECCTA's identity verification regime now has active enforcement behind it, not just a filing obligation firms can quietly overlook. Firms relying on Companies House data for CDD or beneficial-ownership checks should treat this as confirmation that director records are becoming increasingly reliable. At the same time, firms should be mindful that the transition period, which ends for most existing directors around November 2026, is now a live compliance deadline.

City of London Police publishes its first Report Fraud Annual Assessment

On 3 September 2026, the City of London Police published its first [Report Fraud Annual Assessment](#), covering cyber crime and fraud reported across England, Wales and Northern Ireland during 2025/26. Reported losses exceeded £3.2 billion, with investment fraud, romance fraud, payment diversion and courier fraud continuing to be treated as high-harm threats. Abuse of position of trust will also become a new priority area for 2026/27. Investment fraud accounted for £911 million in reported losses, with cryptocurrency involved in around a third of investment fraud reports. Reports identifying AI as an enabler rose from 193 to 956, with criminals using the technology to make scams more convincing through fake celebrity investment promotions and real time AI-generated videos. Invoice fraud remains the most common type of payment diversion, while pension account takeover is identified as an emerging typology.

**WHAT THIS MEANS FOR FIRMS**

Firms should consider whether they are exposed to these typologies, and if their controls are robust enough to identify, detect and prevent fraud. For example, firms should review if their transaction monitoring rules monitor for small, initial payments before larger transfers occur. Additionally, vulnerability controls should be reviewed to detect abuse of position of trust, where seemingly authorised payments stem from customer exploitation.

Issue 37 of SARs in Action

The National Crime Agency (NCA) has published Issue 37 of [SARs in Action](#), covering topics such as UKFIU impersonation, the use of AI to bypass CDD checks, and bribery and corruption threats in the UK. Notably, updated guidance agreed between the FCA and NCA advises that perpetrator financial institutions are better positioned to file detailed SARs on fraud cases, as they hold key details regarding receiving accounts. Consequently, victim financial institutions are no longer expected to file duplicate SARs, helping streamline reporting and focus UKFIU resources on high-priority intelligence.

WHAT THIS MEANS FOR FIRMS

As advised by the NCA, firms should consider the proposal and decide whether to implement any operational changes to reduce duplicative fraud victim SARs. However, this should be in line with the firm's own risk appetite and reporting obligations.

Citibank NA fined £4.7m by OFSI for sanctions violations

The Office of Financial Sanctions Implementation (OFSI) has [fined](#) Citibank N.A. London Branch (CBNA London) £4,732,830.58 for multiple UK financial sanctions breaches involving 970 payments worth approximately £19.72 million. The breaches were primarily related to Russia sanctions and failures to promptly restrict, escalate and report accounts linked to designated persons. Most of the breaches referred to in the notice were from February to November 2022. OFSI reduced the original penalty, reinforcing the expectation that firms should identify and report breaches promptly and provide proactive, meaningful cooperation during investigations.



WHAT THIS MEANS FOR FIRMS

Firms must ensure sanctions screening and escalation processes remain effective under pressure, promptly freeze/restrict accounts following designation, and avoid excessive reliance on manual processes that can create backlogs and human error.

JMLSG publishes final Part I amendments, now awaiting HM Treasury approval

On 3 September 2026, the Joint Money Laundering Steering Group (JMLSG) published [final revisions](#) to Part I of its Guidance, following a consultation that ran from 1 to 29 June 2026. The amendments address:

- Clarification of the use of “unusually”
- a new exception for bank insolvencies
- additional guidance on acting on behalf of a customer
- amendments on pooled client accounts

The revisions are Board-approved but have been submitted to HM Treasury for ministerial approval, which remains outstanding.

WHAT THIS MEANS FOR FIRMS

Until HM Treasury signs off, the changes are not yet approved guidance, so firms should treat them as forthcoming rather than in force. The pooled client account and “acting on behalf of” changes are the likeliest to affect CDD procedures, particularly for firms that hold client money or accept instructions from agents. Firms should compare the revised text against their current CDD and monitoring wording, so any updates can be made quickly once approval lands.

OFSI updates its FAQ on crediting interest on frozen accounts, and Iranian banks

In September 2026, OFSI added two [FAQs](#) to its UK financial sanctions guidance.

- FAQ 203: OFSI confirmed that regulation 58(3) of the Russia (Sanctions) (EU Exit) Regulations 2019, and its equivalents in other regimes including the counter-terrorism regimes, only permits a relevant institution to credit a frozen account with interest or other earnings due on that account. Interest cannot be moved to a different frozen account, even where both belong to the same designated person.
- FAQ 204: This supports new licensing guidance published on 23 September 2026, setting a presumption of denial for licence applications involving five designated Iranian banks: Bank Sepah, Melli Bank plc, Bank Saderat, Persia International Bank and Bank Tejarat. Applications will generally be refused unless there are clear and compelling grounds for an exception. FAQ 204 explains how OFSI will apply that test, citing risk to life or environmental safety, essential regulatory payments, preservation of assets and the orderly wind-down of operations as the kinds of circumstances that may qualify.

OFSI updates its FAQ on crediting interest on frozen accounts, and Iranian banks (continued)

WHAT THIS MEANS FOR FIRMS

FAQ 203 is a practical point for operations and sanctions teams. Interest accrual on frozen balances should be credited back to the same account only, and any process that consolidates or sweeps interest across a designated person's accounts needs close attention. FAQ 204 raises the bar for anyone with Iran-linked exposure. Firms should not plan on licenses being available for dealings with the five banks, and should review any wind-down or payment arrangements that currently rely on case-by-case licensing.

UK consultation on unauthorised fraud

The Home Office's [call for evidence](#) on unauthorised fraud opened on 15 July 2026 and closed on 7 October 2026. It focuses on fraud where transactions are made without the customer's knowledge or consent, including unauthorised card, remote banking and cheque fraud. The figures show why the Government is looking at this: 3.81 million cases were reported in 2025, up 11% on 2024 and 40% on 2023, despite total losses falling 5% to £703.4 million. The call for evidence also treats account takeover as a method or enabler that can cut across different fraud types, rather than a standalone category, and highlights SIM swaps, compromised credentials, digital wallets, synthetic identities and AI-enabled fraud as areas of concern. It also reiterates the Government's intention to remove the existing Strong Customer Authentication requirements from the Payment Services Regulations 2017 and move towards a more flexible, outcomes based approach.

WHAT THIS MEANS FOR FIRMS

The call for evidence has closed and there are no outstanding actions for firms, however the consultation gives a good indication of where Government attention is heading. Firms should review controls around common account takeover routes, particularly changes to contact details or credentials, new-device enrolment, SIM swaps and number ports, and digital wallet provisioning. They should also consider whether any of these journeys rely too heavily on SMS OTPs or other authentication methods that may themselves be compromised.

UK and Cambodia join forces to crackdown on online scam centres

On 23 September 2026, the UK and Cambodia signed a [Memorandum of Understanding](#) to strengthen cooperation against online scam centres. The agreement will increase intelligence and data sharing, support coordinated action against the criminal networks behind these operations, and improve support for victims of trafficking who are forced to carry out scams. The UK will also provide training to Cambodian law enforcement on cyber investigations and digital forensics. The two countries will work through the UK and INTERPOL's Global Fraud Taskforce to identify suspects, dismantle scam centres and trace the illicit financial flows that support them. It was stated that more than two-thirds of fraud affecting the UK originates overseas.



WHAT THIS MEANS FOR FIRMS

The agreement creates no new requirements for firms, but it reinforces the Government's focus on disrupting the overseas networks behind fraud targeting UK customers, rather than looking only at the point where the victim loses money. For firms, the financial flows linked to these networks remain particularly relevant. This includes identifying patterns associated with scam payments and considering whether monitoring looks across a customer's activity over time rather than assessing each payment in isolation. The agreement also follows the UK's 2025 sanctions against scam-centre networks in Southeast Asia, including the Prince Group, which had invested heavily in UK property. This is a reminder that exposure to these networks can extend beyond payments into corporate structures, property and other assets.

EUROPE.

Europol and Spanish police dismantle “Dubai Bank”, a €300m a year underground banking network

On 27 September 2026, Europol [announced](#) it had supported Spanish authorities in dismantling “Dubai Bank”, an underground financial network that Europol said was serving criminal organisations linked to drug trafficking in more than twenty countries. Over 200 officers raided 21 locations across Spain, arresting 21 individuals. The network, composed mainly of Syrian nationals, active since 2020, is believed to have laundered more than €300 million per year; the investigation traces back to the 2021 interception of a cocaine shipment.

WHAT THIS MEANS FOR FIRMS

Although Europol has not yet disclosed the exact money laundering methods used within this network, this lands directly alongside this edition’s global spotlight on hawala and underground banking. It offers a live, large-scale illustration of exactly how that typology can potentially be operated on a large scale, with the network serving criminals across more than twenty countries. Firms with exposure to trade finance, correspondent banking, or payment corridors touching any of those jurisdictions should treat this as a prompt to validate whether their typology library would catch value transfer that never touches a formal hawala-style ledger entry. FATF notes that this hybrid model can be difficult to detect using conventional transaction monitoring. Each stage of a transfer may look routine on its own, and the risk only becomes apparent when the stages are viewed together. Firms should also expect further details on the methodologies used by this network as the case develops, and may wish to revisit this once Europol or Spanish authorities publish more information.

AMLA closes consultations on ongoing monitoring and suspicious activity reporting standards

The EU’s Anti-Money Laundering Authority (AMLA) closed two consultations in September: its [draft Guidelines](#) on ongoing monitoring of business relationships (closed on 3 September 2026) and its [draft Implementing Technical Standards](#) on the format for reporting suspicions and providing transaction records to FIUs (closed 20 September).

The monitoring guidelines explicitly seek input from newly regulated sectors under the recast AML Regulation, including crypto-asset service providers, crowdfunding platforms, and notably football clubs. Final guidelines are expected in Q4 2026.

AMLA closes consultations on ongoing monitoring and suspicious activity reporting standards (continued)

WHAT THIS MEANS FOR FIRMS

This is AMLA's single rulebook taking shape in real time. Both texts will become binding standards rather than guidance firms can take or leave. The ongoing monitoring guidelines will set the bar for what "continuous" transactions and customer information review looks like across the bloc. Firms operating EU entities, or UK firms benchmarking against EU standards, should flag Q4 2026 for revisiting monitoring procedures once the final text lands. The SAR-format ITS (Implementing Technical Standards) is more mechanical but has real operational bite: firms filing into multiple EU jurisdictions should expect a harmonised reporting template to replace today's patchwork of national formats, which has implications for case management and SAR drafting workflows.

European Commission opens infringement proceedings against 18 Member States over AMLD6 transposition gaps

On 25 September 2026, as part of its monthly infringement package, the European Commission sent [letters of formal notice](#) to 18 Member States (Belgium, Bulgaria, Czechia, Germany, Estonia, Greece, Spain, France, Croatia, Cyprus, Lithuania, Luxembourg, the Netherlands, Austria, Poland, Portugal, Romania and Finland) for failing to notify transposition of provisions in the sixth Anti-Money Laundering Directive (EU) 2024/1640. The provisions at issue govern access to beneficial ownership registers for competent authorities, self-regulatory bodies, and obliged entities, with a transposition deadline of 10 July 2026. The affected states now have two months to respond; the Commission has stated that a reasoned opinion may follow if the responses are unsatisfactory.

WHAT THIS MEANS FOR FIRMS

Beneficial ownership register access is foundational to CDD and source-of-wealth checks, and this gap means the practical reality of what firms can actually pull from national registers will keep diverging across these 18 jurisdictions well past the directive's nominal deadline. Firms relying on registry access as part of their CDD process for entities incorporated in any of the named states should not assume AMLD6-level transparency is live yet, and should keep verifying register functionality jurisdiction-by-jurisdiction rather than treating the July deadline as the operative date. This would be worth revisiting following the close of the two-month window in late November 2026.

US.

US Treasury designates VTB Bank for facilitating Iran's sanctions evasion

On 14 September 2026, the US Treasury's Office of Foreign Assets Control (OFAC) **designated** VTB Bank, one of Russia's largest financial institutions, under Operation Economic Outcast. The Treasury's designation describes VTB as having opened offices in Iran, established correspondent relationships with sanctioned Iranian financial institutions, and built a settlement system using correspondent accounts in Iranian rials and Russian rubles to move billions of dollars in frozen Iranian assets. The designation blocks all VTB property and interests in property subject to US jurisdiction, extends to entities 50% or more owned by VTB, and exposes any foreign financial institution that knowingly facilitates significant VTB transactions to secondary sanctions.



WHAT THIS MEANS FOR FIRMS

The direct relevance here is unlikely to be a UK payment firm's own relationship with VTB. However, this is a clear, current illustration of how the US uses correspondent-account architecture as both the evasion tool (Russia-Iran settlement via correspondent accounts) and the enforcement lever (secondary sanctions risk for any institution found facilitating it). Firms with correspondent banking relationships, or that rely on intermediary banks to reach certain corridors, should treat this as a prompt to check how exposure to a newly designated institution would surface through a nested or downstream relationship, not only through a direct one, and to confirm that sanctions screening is applied.

FinCEN alert: money laundering tied to overseas “scam centre” investment fraud

On 3 September 2026 the Financial Crimes Enforcement Network (FinCEN) issued [Alert FIN-2026-Alert005](#) and an accompanying Financial Trend Analysis identifying nearly \$13 billion in suspected Bank Secrecy Act-reported activity linked to digital-asset investment scams (commonly known as “pig butchering”) run from overseas scam centres, predominantly in Southeast Asia. The alert sets out red flags across the lifecycle of these schemes: victim-facing romance or investment-relationship grooming, conversion of victim funds into cryptocurrency, and layering of proceeds through a mix of exchanges, shell companies and trade-based channels before cash-out.



WHAT THIS MEANS FOR FIRMS

The alert gives firms something concrete to test for, beyond a general typology of which to be aware. The alert's red flags translate into specific transaction-monitoring scenarios: a customer making escalating transfers to a crypto exchange shortly after opening or reactivating an account, particularly where the stated purpose of the account doesn't match investment activity; payments to newly created or recently changed-purpose business accounts that act as a pass-through to crypto exchanges; and victims who increase transfer amounts over time under pressure from a counterparty they have not met in person. Firms handling retail payments or acting as an on-ramp to crypto exchanges should check these specific patterns against their existing fraud and AML typology libraries, rather than only against generic “crypto-related” risk indicators.

US Treasury cracks down on transnational criminal organisation behind cyber scam operations targeting Americans

On 9 September 2026, OFAC [designated](#) Xinbi Guarantee as a significant transnational criminal organisation. Xinbi operates a Chinese-language online marketplace connecting scam centre operators and money laundering networks with merchants providing financial services, technology and other goods, and also provides escrow services through the platform. Treasury says Xinbi has processed more than \$24 billion in digital assets and fiat currency since around 2022 and has been used by North Korean hackers and entities linked to Jin Bei Group and the Prince Group. OFAC also designated SafeW Technology, which developed the encrypted messaging platform used by Xinbi, and Anwen Technology, which developed its XinbiPay crypto wallet. The Department of Justice also seized infrastructure and digital asset wallets used by Xinbi on the same day. The UK had already sanctioned Xinbi in March 2026, becoming the first country to do so.



WHAT THIS MEANS FOR FIRMS

Firms with US sanctions exposure should ensure Xinbi, SafeW Technology and Anwen Technology are captured within screening lists, along with any entities caught by OFAC's 50% ownership rule. Xinbi is also already subject to UK sanctions. The action shows how quickly these networks can move when enforcement catches up with them. Treasury notes that activity shifted from Huione to Xinbi following regulatory action, while Xinbi itself moved users onto new messaging and wallet infrastructure as scrutiny increased. For firms with crypto exposure, blockchain analytics and transaction monitoring should therefore consider exposure to wallets and services linked to these networks, including where activity moves onto newly identified platforms following enforcement action, rather than relying only on names and wallet addresses already appearing on sanctions lists.

END-TO-END SUPPORT FOR YOUR FINANCIAL CRIME COMPLIANCE PROGRAMME.

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.

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

-
- 01 Audits and Assurance**
Independent firm-wide financial crime audits (AML, CTF, sanctions, fraud), targeted assurance and health checks

 - 02 Control Enhancements and Implementation**
Building and optimising control areas including customer due diligence, screening, transaction monitoring and investigations

 - 03 Risk Assessment**
Enterprise-wide financial crime risk assessments, risk appetite, and customer risk assessments

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

 - 05 Remediations and Regulatory Enforcement Support**
Expert guidance on engaging with the regulator, plus planning and executing effective remediation projects
-

contact@fintrail.com · www.fintrail.com