FINTRAIL

A COSEGIC COMPANY

# REGCAP

## OCTOBER 2026

A summary of the latest FinCrime regulatory news

WWW.FINTRAIL.COM CONTACT@FINTRAIL.COM

# GLOBAL.

## FinCEN, OFAC and the UK move against the A7 sanctions evasion network

On 1 October 2026, the US Financial Crimes Enforcement Network (FinCEN) issued an alert on the A7 Network, a Russia-linked shadow banking network used to facilitate sanctions evasion and money laundering for actors including Iran, North Korea and cybercriminal groups. FinCEN identified hundreds of companies operating across at least 83 countries as intermediaries, known as Sub-Agents, which disguise the involvement of sanctioned entities in international payments. The network uses falsified trade documentation, including invoices altered using AI, and the ruble-backed stablecoin A7A5 to move funds while concealing their origin. Alongside the alert, FinCEN proposed restrictions on transactions involving the network's Sub-Agents, while the Office of Foreign Assets Control (OFAC) designated the network as a significant transnational criminal organisation. On 8 October 2026, the UK announced new sanctions against three cryptocurrency exchanges and two payment platforms suspected of facilitating Russian sanctions evasion, including two linked to A7 transactions.

### WHAT THIS MEANS FOR FIRMS

Firms should review their exposure to the A7 Network and associated intermediaries, particularly where payments involve third-country entities with unclear ownership structures or limited commercial justification. Transaction monitoring and sanctions screening should account for the indicators identified by FinCEN, including unusual payment routing, inconsistencies in trade documentation and exposure to A7A5 or associated cryptocurrency services. Where firms have dealt with the newly designated platforms, they should assess whether any previous transactions involved parties already subject to sanctions at the time and ensure current sanctions restrictions are applied. The proposed US transaction restrictions are not yet final, but the OFAC and UK sanctions measures are already in effect.

## FATF removes four jurisdictions from its grey list

The Financial Action Task Force (FATF) concluded its October plenary on 30 October 2026, the first under the UK Presidency of Giles Thomson. It removed Bulgaria, Côte d'Ivoire, the Democratic Republic of the Congo and Monaco from its list of jurisdictions under increased monitoring (the grey list) after on-site visits confirmed they had completed their action plans, and added none, leaving 18 jurisdictions on the list. The list of high-risk jurisdictions subject to a call for action is unchanged: North Korea and Iran remain subject to countermeasures, and Myanmar to enhanced due diligence. The plenary also agreed to accelerate implementation of the FATF standards on virtual assets in jurisdictions with materially important virtual asset activity, through a targeted review with results due in 2027, and approved a report on illicit financial flows linked to scam compounds. It adopted the mutual evaluation reports for Mexico and the United States, which are due to be published in December 2026. The plenary outcomes are on the FATF website.

## FATF removes four jurisdictions from its grey list (continued)

### WHAT THIS MEANS FOR FIRMS

Firms should update country risk ratings to reflect the four removals, but should consider if they want to drop all enhanced measures automatically or take a phased approach: customers and counterparties with links to Bulgaria, Côte d'Ivoire, the Democratic Republic of the Congo and Monaco could still be assessed on their own risk. The call for action list is unchanged, so existing controls for North Korea, Iran and Myanmar remain in place. UK and EU lists of high-risk third countries may be amended to follow the FATF changes, so firms should watch for updates from HM Treasury and the European Commission. The focus on virtual assets and scam compounds signals continued attention to crypto flows and fraud proceeds.

## Australian Federal Court orders Star to pay $183 million for AML/CTF failings



On 28 October 2026, the Federal Court of Australia ordered Star Sydney and Star Queensland, casino operators in The Star Entertainment Group, to pay AUD 260 million (approximately US$183 million) in civil penalties (AUD 195 million and AUD 65 million respectively) in proceedings brought by the Australian Transaction Reports and Analysis Centre (AUSTRAC), as reported by Lawyers Weekly. The court found that the casinos failed to maintain a compliant anti-money laundering and counter-terrorism financing (AML/CTF) programme and failed to carry out ongoing customer due diligence (CDD), with breaches on 1,190 occasions at Star Sydney and 327 at Star Queensland. Senior management had been warned that some customers were likely linked to organised crime and money laundering, yet the business continued to court high-risk customers. AUSTRAC had sought about AUD 400 million, but the court reduced the penalty to reflect action already taken by state regulators, including AUD 200 million in penalties already paid, and the remediation under way.

### WHAT THIS MEANS FOR FIRMS

Gambling operators, and the banks and payment providers that serve them, should test whether high-risk customers receive enhanced monitoring and source of funds checks in practice, and whether management information shows how many high-risk customers are retained against compliance advice. Commercial priorities should not override escalation and exit decisions. The judgment shows that penalties from other regulators may be taken into account but do not remove the risk of a significant penalty from the AML supervisor.

# UK.

## FCA restricts six Annex 1 firms over anti-money laundering controls

On 23 October 2026, the Financial Conduct Authority (FCA) announced restrictions on six unregulated lenders, known as Annex 1 firms, following concerns about their AML policies, controls and procedures. The firms include Kingscrown Finance Ltd, MOMSB Ltd, Momentus Capital Ltd, Grosvenor Funding Ltd, Grosvenor Funding (North West) Ltd and Abbital Ltd. The restrictions, imposed by the FCA at the firms' request between April and October 2026, limit their ability to onboard new customers, enter into new lending arrangements or accept certain payments from existing customers. Five of the firms are also required to undergo independent reviews of their AML frameworks, while Kingscrown Finance must wind down its existing loan book. The FCA reiterated its increased scrutiny of Annex 1 firms, which are registered for AML supervision but are not otherwise FCA-authorised, and confirmed it is reviewing responses to information requests sent to approximately 900 registered firms. This follows the FCA's August 2026 warning regarding increased supervision of the sector.

### WHAT THIS MEANS FOR FIRMS

Annex 1 firms should ensure their AML risk assessments, policies and controls are tailored to their individual business models and risks, rather than relying solely on group-level arrangements. The FCA's intervention reinforces its willingness to impose business restrictions where firms cannot demonstrate effective financial crime controls. Regulated firms dealing with Annex 1 entities should also review their counterparty due diligence, including independently verifying registration status, understanding the nature of the firm's activities and assessing associated financial crime risks.

Read our blog post: FCA restricts six Annex 1 firms over anti-money laundering controls

## FCA signals a shift from activity to effectiveness in financial crime supervision

At its Annual Public Meeting on 6 October 2026, the FCA indicated that financial crime would become an even greater supervisory priority, reflecting the evolving threat landscape and increasing use of technology by criminals. As reported by AML Intelligence, the following day Beth Harris, Head of the FCA's financial crime department, said that financial crime frameworks have historically placed too much emphasis on completing compliance activities rather than demonstrating their effectiveness, and warned against policies, procedures and controls that exist only on paper, without evidence that they prevent financial crime. The FCA is increasingly focused on whether controls operate effectively in practice, whether weaknesses are identified and addressed, and whether firms can demonstrate that their frameworks make it harder for criminals to exploit the financial system.

## FCA signals a shift from activity to effectiveness in financial crime supervision (continued)

### WHAT THIS MEANS FOR FIRMS

Firms should review how they assess and evidence the effectiveness of their financial crime controls, rather than relying solely on demonstrating that required processes have been completed. Management information should provide insight into control performance, including the effectiveness of transaction monitoring, quality assurance findings, identified weaknesses and remediation outcomes. Firms should also ensure that lessons from investigations, control failures and emerging risks feed back into their financial crime frameworks. This reinforces the FCA's broader supervisory focus on proportionate, risk-based controls that demonstrably prevent and disrupt financial crime.

## FCA consults on updates to its Financial Crime Guide

On 23 October 2026, the FCA opened a consultation (CP26/38) on proposed updates to its Financial Crime Guide. The proposals cover fraud, cryptoassets (to reflect the new cryptoasset regime that takes effect in October 2027), financial and trade sanctions, proliferation financing, data security, financial crime systems and controls, and money laundering and terrorist financing. The consultation is relevant to all firms the FCA supervises for financial crime, including Annex 1 firms and cryptoasset businesses, and closes on 24 December 2026.

### WHAT THIS MEANS FOR FIRMS

Firms should read the proposed changes against their own policies and controls to identify gaps, particularly on sanctions, systems and controls and, for cryptoasset businesses, the new regime. The FCA will publish the final text in a policy statement after considering responses. It has not yet said when the changes would take effect, so firms should consider responding by 24 December 2026 to help shape the outcome.

## UKFIU publishes SARs Annual Report 2025 to 2026



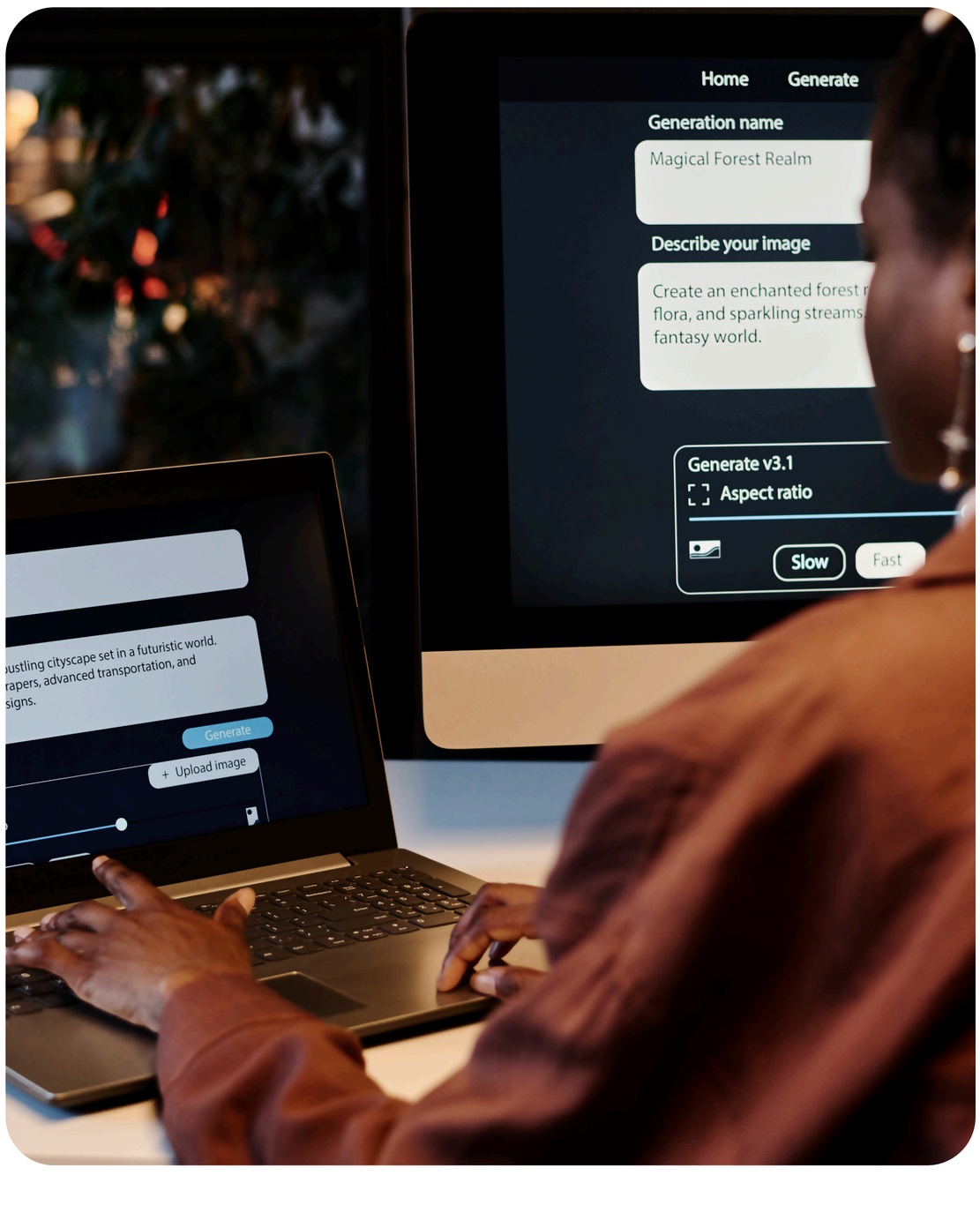

On 16 October 2026, the UK Financial Intelligence Unit (UKFIU), part of the National Crime Agency (NCA), published its SARs Annual Report 2025 to 2026, highlighting developments in suspicious activity reporting and asset recovery. The UKFIU received 896,414 suspicious activity reports (SARs), a 3.4% increase on the previous year, while requests for a Defence Against Money Laundering (DAML) fell by 23% to 44,553. The decline was largely attributed to the July 2025 increase in the relevant DAML exemption threshold from £1,000 to £3,000. Despite fewer requests, the total value of assets denied through the DAML regime increased by 15% to £440.8 million, including £422.3 million associated with refused requests. This brings the total value of assets denied over the past three years to more than £1 billion. Banks accounted for 84.83% of SARs submitted through the SAR Portal, with the UKFIU highlighting improvements in reporting quality as contributing to stronger asset denial outcomes.

### UKFIU publishes SARs Annual Report 2025 to 2026 (continued)

**WHAT THIS MEANS FOR FIRMS**

Firms should review their SAR and DAML procedures to ensure the revised £3,000 threshold is correctly applied to eligible transactions, while recognising that the underlying obligation to report suspicious activity remains unchanged. The report reinforces the importance of submitting high-quality, actionable intelligence rather than focusing solely on reporting volumes. Firms should ensure SARs clearly document the grounds for suspicion, relevant transaction details and associated parties, and that DAML requests contain sufficient information to support timely law enforcement decisions. Regular quality assurance and feedback from the UKFIU should also be incorporated into reporting procedures to improve the effectiveness of financial crime controls.

## FCA publishes good and poor practice for AI in financial services




On 19 October 2026, the FCA published examples of good and poor practice for firms developing, deploying or using AI, drawing on supervisory work, industry engagement and its AI Lab initiatives. The publication focuses on consumer outcomes, governance and accountability, and operational resilience, highlighting the importance of effective oversight throughout the AI lifecycle. Good practice includes assigning clear senior management accountability, conducting structured testing and approval before deployment, maintaining documented decision-making and escalation processes, and monitoring AI performance and outcomes. Areas for improvement include unclear responsibilities, inadequate documentation, excessive reliance on technical teams or third-party providers, and human oversight that becomes a box-ticking exercise rather than meaningful scrutiny. The FCA also highlights the importance of testing AI systems for bias, including where they influence fraud detection or decisions affecting vulnerable customers. The examples are illustrative and do not introduce new regulatory requirements.

**WHAT THIS MEANS FOR FIRMS**

Firms using AI in financial crime activities, including transaction monitoring, sanctions screening, customer onboarding and fraud detection, should consider whether their existing governance arrangements provide sufficient oversight and accountability.

This includes clearly defined ownership, documented testing and validation, monitoring for model performance and unintended outcomes, and appropriate human review of AI-generated decisions. Firms should also ensure that third-party AI solutions are subject to proportionate due diligence and ongoing oversight, rather than relying solely on vendor assurances. The FCA's findings reinforce that firms remain accountable for the effectiveness and outcomes of AI systems, regardless of whether they are developed internally or outsourced.

## FCA sets out plans to use AI agents in supervision

On 19 October 2026, Jessica Rusu, the FCA's chief data, information and intelligence officer, said in a speech at the Bloomberg UK Policy Series that the FCA is building AI tools, including AI agents, to supervise the roughly 60,000 AML firms that will come into its remit in 2028. The FCA plans to use an AI agent to supervise about 9,000 small wholesale markets transaction reporting firms, and use AI to gather evidence, combine intelligence from several sources and flag early warning signs. Rusu said a joint FCA and Bank of England survey, due to be published the following week, shows that 86% of firms use AI. She also set out how the FCA is acting on the Mills Review, which the FCA commissioned and published in July 2026, on AI in retail financial services to 2030. The speech indicates direction and does not create new requirements for firms.




### WHAT THIS MEANS FOR FIRMS

Firms already supervised by the FCA should expect regulatory data to be analysed at scale, so the accuracy and consistency of what they submit matters more. Firms that will come into FCA AML supervision in 2028 should prepare for data-led, increasingly automated supervision. Firms using AI in their own controls should expect questions on governance, oversight and explainability, in line with the FCA's good and poor practice examples above.

## UK sanctions packages target Russian LNG, oil and crypto facilitators

On 1 October 2026, the UK Government announced 31 new sanctions measures against Russia, targeting its liquefied natural gas (LNG) shadow fleet, disinformation networks, and individuals involved in human rights abuses in occupied Ukraine. The measures covered 22 individuals, one entity (Novatek Gas and Power Asia Pte Ltd), and eight vessels.

### UK sanctions packages target Russian LNG, oil and crypto facilitators (continued)

The UK also introduced two time-limited general trade licences permitting certain LNG transportation activities involving Japan and South Korea under existing contracts between January 2027 and March 2028. On 8 October, the Government announced a further 38 sanctions measures, including Russian oil companies Zarubezhneft and INK Capital, 12 shadow fleet tankers, 17 suppliers of military-related goods, and three cryptocurrency exchanges and two payment platforms suspected of facilitating sanctions evasion. Two of the financial platforms were linked to transactions involving the A7 Network. The UK stated that its sanctions now cover over 90% of Russia's oil production capacity, with more than 600 shadow fleet oil tankers sanctioned.

**WHAT THIS MEANS FOR FIRMS**

Firms should ensure sanctions screening systems are updated to reflect the latest designations and assess potential exposure across customers, counterparties and associated ownership structures. Those involved in trade finance, shipping or insurance should review their exposure to Russian energy transactions, including designated vessels and the conditions attached to any applicable trade licences. Firms should also consider historical transactions involving newly sanctioned cryptocurrency exchanges and payment platforms to identify potential exposure to previously sanctioned entities or suspicious activity. Where designated persons or their assets are identified, firms must apply the relevant restrictions, including asset freezes and reporting to the Office of Financial Sanctions Implementation (OFSI), where required.

## CPS secures an unexplained wealth order over about £50 million of assets

On 23 October 2026, the Crown Prosecution Service (CPS) announced that the High Court had granted an unexplained wealth order (UWO) and an interim freezing order under the Proceeds of Crime Act 2002 against two British nationals and associated companies. The orders freeze assets worth about £50 million, including properties in England, France, Spain and Portugal, a yacht, vehicles and a bank account. The CPS alleges that the assets derive from international illicit funds laundered in the UK. The respondents have three months to show that the assets were lawfully obtained, failing which the CPS may seek a civil recovery order. They have not been charged with or convicted of any offence.

**WHAT THIS MEANS FOR FIRMS**

Firms should be ready to apply the terms of any freezing order to accounts they hold, and to take legal advice if they identify a link to the respondents or the frozen assets. The case is a reminder to test source of wealth evidence for high-value property, yacht and cross-border asset purchases, and to consider whether a SAR is required where that evidence is weak.

# EUROPE.

## DNB fines Modulr Finance B.V. over customer due diligence failings

On 5 October 2026, De Nederlandsche Bank (DNB) announced a €722,160 fine against Modulr Finance B.V., a Dutch electronic money institution (EMI), for serious deficiencies in its AML controls between January 2023 and July 2024. DNB found that Modulr relied heavily on intermediary partners, including crypto-asset service providers, to conduct ongoing customer and transaction monitoring, leaving the firm with insufficient oversight of its own customer base. Its transaction monitoring systems failed to adequately identify high-risk activity, including transactions involving high-risk jurisdictions, non-resident customers and unusual payment patterns. Monitoring thresholds were also set too high, meaning that large cumulative amounts involving multiple smaller transactions did not trigger alerts. As a result, indicators of potential money laundering and fraud were either missed or identified and reported too late. DNB treated Modulr's remediation and cooperation as mitigating factors, including improvements to its monitoring framework and restrictions on relationships with three of its four relevant partners. Modulr also accepted the facts underlying the violation and the fine and agreed not to object, so DNB reduced the original €849,600 fine by 15% under its simplified settlement procedure.

### WHAT THIS MEANS FOR FIRMS

Firms relying on agents, distributors or other intermediaries for AML activities should ensure they maintain sufficient oversight of their own customers and transactions, as responsibility for effective ongoing monitoring remains with the regulated institution. This includes maintaining appropriate customer risk profiles, setting transaction monitoring thresholds that reflect underlying customer activity, and ensuring suspicious activity is investigated and escalated promptly. Firms should also regularly assess the effectiveness of their monitoring arrangements and the quality of information received from intermediaries. The enforcement action is particularly relevant to EMIs and payment service providers operating partner-led or embedded finance models, where reliance on third parties can create gaps in customer visibility and financial crime controls. The reduction also shows the value of cooperating with the regulator: firms that face enforcement in future should expect early remediation, acceptance of the facts and constructive engagement to count in their favour.

## Commission sets common formats for beneficial ownership information

On 22 October 2026, the European Commission published Implementing Regulation (EU) 2026/2354, establishing standardised formats for submitting beneficial ownership information to national registers across EU Member States. The regulation forms part of the EU's broader AML framework and aims to improve the consistency, quality and interoperability of beneficial ownership data. It introduces common reporting formats covering beneficial owner identification, ownership and control structures, legal entities, trusts and nominee arrangements.

### Commission sets common formats for beneficial ownership information (continued)

Firms with complex ownership structures will also be required to provide information illustrating the relationships between entities and their ultimate beneficial owners. National registers will be required to apply minimum information requirements when accepting submissions, helping reduce incomplete or inconsistent records. The regulation will apply from 10 July 2027.

**WHAT THIS MEANS FOR FIRMS**

No direct action; the changes do not introduce new requirements for financial institutions conducting CDD, but support more consistent beneficial ownership transparency across the EU. Greater consistency in register data may support beneficial ownership checks across jurisdictions. Regulated firms must continue to report beneficial ownership discrepancies in accordance with existing applicable national requirements.

## AMLA finalises three technical standards under the Anti-Money Laundering Regulation

On 1 October 2026, the EU's Anti-Money Laundering Authority (AMLA) announced the finalisation of three draft regulatory technical standards (RTS) under the Anti-Money Laundering Regulation (EU) 2024/1624, which will apply from 10 July 2027. The CDD standard sets out the information to collect for standard, simplified and enhanced due diligence, the reliable sources firms can use to verify identity, and the attributes that electronic identification must have. The second standard sets out how to identify business relationships, occasional transactions and linked transactions, and where a lower CDD threshold should apply for higher-risk firms, sectors or transactions. The third covers group-wide requirements, including minimum policies, controls and information sharing across a group, and the additional measures firms must take where the law of a third country prevents compliance with the Regulation. The final drafts have been submitted to the European Commission for adoption and are proposed to apply six months after entering into force.

**WHAT THIS MEANS FOR FIRMS**

Firms with EU operations should review their existing CDD procedures, transaction assessment criteria and group-wide AML frameworks against the proposed standards to identify potential gaps ahead of implementation. Particular attention should be given to identifying linked transactions, applying proportionate customer verification measures and ensuring effective oversight of subsidiaries operating outside the EU. UK-based groups with EU entities should also assess whether their group-wide policies and information-sharing arrangements will meet the new requirements. As the standards remain subject to formal adoption by the European Commission, firms should monitor their progress and prepare for implementation rather than treating the draft requirements as already in force.

## AMLA consults on a central EU AML database

On 7 October 2026, AMLA published a consultation on draft RTS under Article 11(6) of Regulation (EU) 2024/1620 for a central EU AML/CFT database. The database would be a single platform on which supervisors and self-regulatory bodies report and access information on supervised entities, supervisors and supervisory activity, supporting information sharing across the EU and more targeted, risk-based supervision. The draft specifies the information to be reported, including money laundering and terrorist financing risks, sanctions and administrative measures, and authorisations and fit and proper assessments. A public hearing is scheduled for 3 November 2026. The draft indicates that the database should add no reporting costs for firms subject to AML obligations.

**WHAT THIS MEANS FOR FIRMS**

No immediate action. Firms with EU supervisors may wish to respond to the consultation or attend the hearing, but the database is a supervisory tool and the draft does not add reporting obligations for firms.

## EU adds 826 entities and 743 individuals to its Russia asset-freeze list



On 12 October 2026, the Council of the European Union adopted Implementing Regulation (EU) 2026/2281, adding 826 Russian companies and 743 individuals to its sanctions list under Regulation (EU) No 269/2014. This represents the largest single set of sanctions listings adopted by the EU, bringing the total number of designated individuals and entities under the regime to nearly 4,600. The measures primarily target companies operating within Russia's military-industrial complex, extending sanctions beyond major defence manufacturers to the wider supply chains supporting Russia's military activities including suppliers of semiconductors, electronics, communications equipment, ammunition and components used in missiles, drones and aircraft. The listed individuals are executives of these companies. The newly designated individuals and entities are subject to asset freezes and prohibitions on making funds or economic resources available to them, directly or indirectly. The regulation entered into force on 12 October 2026.

**WHAT THIS MEANS FOR FIRMS**

Firms with exposure to EU sanctions should ensure their screening systems reflect the new designations. Firms should also assess ownership and control relationships to identify potential indirect exposure to sanctioned parties. Particular attention should be given to firms involved in trade finance, correspondent banking and payments linked to Russian industrial supply chains, where previously permissible transactions may now involve designated entities. Any identified exposure should be assessed against applicable asset-freezing and reporting obligations.

# US.

## Bank of America pays $1.2 billion in coordinated AML penalties

On 13 October 2026, the Financial Crimes Enforcement Network (FinCEN) announced a $1.2 billion civil money penalty against Bank of America, N.A., for widespread AML deficiencies between January 2018 and July 2025. The penalty includes a $750 million fine imposed by the Office of the Comptroller of the Currency (OCC), the largest in its history. FinCEN found that the bank's transaction monitoring system relied on poorly calibrated risk scores and a 20-point threshold before potentially suspicious activity was escalated for investigation, resulting in significant delays and missed suspicious activity. The deficiencies contributed to more than $5 billion in suspicious transactions being missed or reported late, while a subsequent review identified nearly 8,900 suspicious activity reports (SARs) that had not been filed, involving approximately $4 billion in transactions. In some years, more than a third of investigations were triggered by external referrals, including law enforcement requests, rather than the bank's own monitoring controls. The bank admitted to wilful violations of the Bank Secrecy Act (BSA), while OFAC separately announced an $11.7 million settlement for apparent sanctions violations.

### WHAT THIS MEANS FOR FIRMS

Firms should review the effectiveness of their transaction monitoring systems, particularly whether risk scoring methodologies, alert thresholds and escalation processes are appropriately calibrated to identify suspicious activity. Regular testing should assess potential false negatives, delays between suspicious activity and reporting, and whether investigations are disproportionately triggered by external referrals rather than internal controls. Firms should also ensure that identified control weaknesses are promptly remediated and that senior management receives sufficient information to challenge monitoring effectiveness. Although the enforcement action concerns US requirements, the findings reinforce the importance of demonstrably effective financial crime controls, consistent with global regulators' increasing focus on outcomes rather than compliance activity alone.

## OCC fines American Express National Bank $350 million over AML failings

On 8 October 2026, the OCC announced a $350 million civil money penalty and cease-and-desist order against American Express National Bank for significant deficiencies in its BSA and AML compliance programme. The OCC found that the bank's AML risk assessment focused disproportionately on its relatively limited deposit products, failing to adequately assess the risks associated with its much larger credit and charge card businesses. Additional weaknesses included insufficiently experienced compliance staff, inadequate CDD and identification procedures, ineffective internal controls, and shortcomings in independent testing and training. These deficiencies contributed to systemic failures in suspicious activity monitoring and reporting, resulting in approximately $13 billion of suspected trade-based money laundering activity over the past decade not being identified, assessed or reported in a timely and sufficient manner. The Federal Reserve Board also issued a concurrent cease-and-desist order against American Express Company and American Express Travel Related Services Company, identifying weaknesses in the group's enterprise-wide AML framework.

## OCC fines American Express National Bank $350 million over AML failings (continued)

### WHAT THIS MEANS FOR FIRMS

Firms should ensure their AML risk assessments adequately reflect the risks associated with all products, services and customer segments, particularly where certain business lines account for a significant proportion of activity. Transaction monitoring controls should be appropriately designed and calibrated to identify relevant money laundering typologies, including trade-based money laundering where applicable. Firms should also assess whether CDD information effectively informs monitoring, and whether compliance functions have sufficient resources and expertise to investigate and escalate suspicious activity. The enforcement action reinforces the importance of aligning financial crime controls with a firm's actual risk exposure, rather than relying on frameworks that do not adequately reflect its business model.

## FinCEN withdraws proposed rules on unhosted wallets and crypto mixing




On 5 October 2026, FinCEN announced the withdrawal of two proposed rules on convertible virtual currency (CVC). The first would have introduced recordkeeping, verification and reporting requirements for certain transactions involving CVC and unhosted wallets. The second would have designated CVC mixing as a class of transactions of primary money laundering concern. FinCEN said it had considered the public comments and that the withdrawals form part of the administration's deregulatory agenda and its efforts to make digital asset regulation fit for purpose.

### WHAT THIS MEANS FOR FIRMS

The proposals were never in force, so existing US obligations are unchanged. UK firms should note that the withdrawal does not alter their own obligations, and that exposure to mixers and unhosted wallets remains a relevant risk factor in customer and transaction risk assessments.

## US steps up Iran-related pressure on financial institutions



Throughout October 2026, the US Department of the Treasury announced further sanctions targeting Iran's financial networks and key economic sectors under Operation Economic Outcast. On 1 October, OFAC expanded the sectors eligible for sanctions under Executive Order 13902 to include Iran's automotive and rail industries, alongside designations targeting companies and foreign suppliers supporting these sectors. On 5 October, OFAC issued a notice warning foreign financial institutions of the risk of secondary sanctions for continuing to conduct business with sanctioned Iranian financial institutions, including potential restrictions on access to the US financial system. Further sanctions announced on 8 October targeted 17 vessels and associated companies involved in transporting Iranian petroleum and petrochemicals through its shadow fleet. On 15 October, Treasury announced additional designations against Iran-linked financial networks, including Iraq Development Bank and offshore financial intermediaries facilitating sanctions evasion. OFAC later issued a general licence authorising transactions needed to wind down dealings with the bank until 1 December 2026. The US State Department also designated Cuba's state-owned Banco Internacional de Comercio S.A. (BICSA), citing its provision of financial services to the previously sanctioned Iranian Karafarin Bank since at least 2022.

### WHAT THIS MEANS FOR FIRMS

Financial institutions, including those operating outside the US, should reassess their exposure to Iranian financial institutions, particularly through correspondent banking relationships, intermediary banks and third-country payment arrangements. Firms involved in trade finance, shipping or energy-related transactions should also review their exposure to newly designated entities and vessels, including indirect ownership and control relationships. OFAC's warning reinforces the importance of understanding secondary sanctions risks, as non-US institutions may face restrictions on access to the US financial system for certain dealings with sanctioned Iranian entities. Firms should ensure their sanctions screening and due diligence arrangements can identify indirect exposure through intermediaries and apply the relevant restrictions where required.

## President waives new Russia sanctions and tariffs under the Graham Act

On 16 October 2026, the US President issued Executive Order 14436, waiving the application of extensive sanctions and tariffs introduced under the Lindsey O. Graham Sanctioning Russia and Iran Act of 2026, which was signed into law on 18 September.

### President waives new Russia sanctions and tariffs under the Graham Act (continued)

The waivers cover proposed tariffs of 500% on Russian imports and 100% on goods from major purchasers of Russian oil and gas, alongside sanctions targeting Russian government-affiliated financial institutions, funds transfers involving Russia, investment activities and the Russian energy sector. The measures have been waived on national interest grounds, with no fixed expiry date, and may be reinstated if circumstances change. The order does not affect existing US sanctions imposed under other authorities or the Act's extension of Iran-related sanctions. Separately, on 9 October, OFAC issued General License 135, authorising certain transactions involving the sale, delivery and importation of Russian-origin diesel fuel until 7 April 2027, subject to specified restrictions.

**WHAT THIS MEANS FOR FIRMS**

Firms should continue applying existing Russia-related sanctions controls, as the waivers do not remove previously imposed restrictions or affect UK and EU sanctions regimes. Firms with exposure to Russian financial institutions, trade finance or energy-related transactions should monitor developments, particularly as the waived measures may be reinstated without a fixed implementation timetable. Those considering transactions under General License 135 should ensure the activities fall within its permitted scope and assess whether other sanctions or statutory restrictions continue to apply, including the separate US prohibition on Russian petroleum imports. The developments highlight the importance of maintaining up-to-date sanctions procedures and distinguishing between existing restrictions, newly waived measures and specific licensing exemptions.

## OFAC sanctions Cartel del Noreste money laundering businesses



On 13 October 2026, OFAC announced sanctions against four individuals and 11 entities connected to Cartel del Noreste (CDN), a Mexico-based drug trafficking organisation designated by the US as a Foreign Terrorist Organisation. The measures target businesses operating across quarter horse racing, construction, trucking and the oil and gas sector, which Treasury identified as supporting the cartel's financial and criminal operations. The action builds on previous sanctions against CDN and highlights how criminal organisations exploit legitimate commercial activities to conceal illicit financial flows and sustain their operations. The designated individuals and entities are subject to US asset-freezing measures and transaction restrictions.

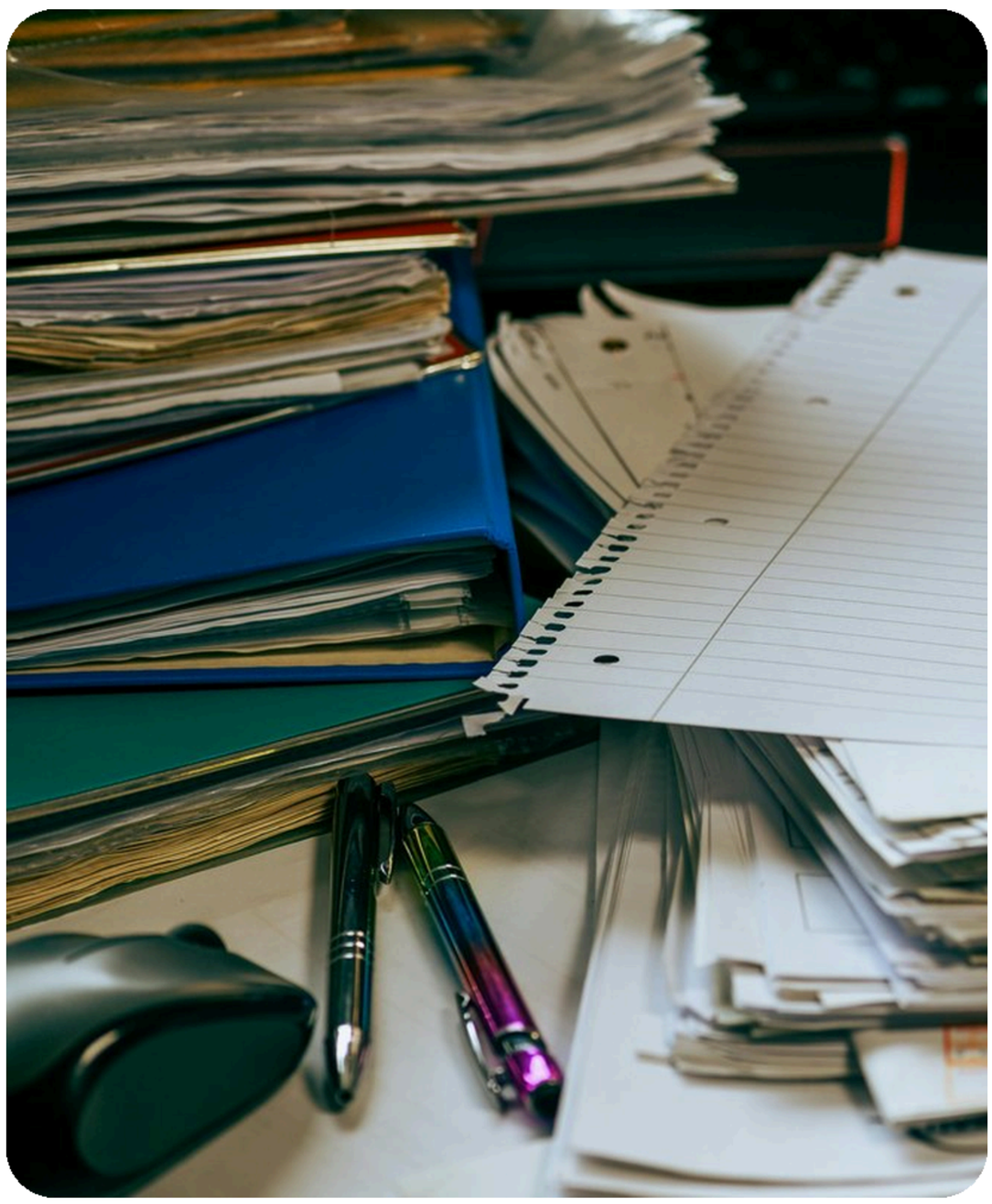
## OFAC sanctions Cartel del Noreste money laundering businesses (continued)

**WHAT THIS MEANS FOR FIRMS**

Firms should ensure their sanctions screening systems reflect the new designations and assess potential exposure through associated businesses and ownership structures. Financial institutions with exposure to sectors such as horse racing, construction, transportation and fuel distribution should consider whether their due diligence and transaction monitoring controls can identify unusual funding arrangements, opaque ownership structures or activity inconsistent with legitimate business operations. The action reinforces the importance of understanding the underlying commercial purpose of transactions and identifying potential connections between apparently legitimate businesses and organised criminal networks.

## OFAC sanctions facilitators of North Korean IT worker schemes

On 28 October 2026, OFAC designated ten individuals and one entity linked to North Korean government IT worker schemes. They include two Russian financial intermediaries who converted cryptocurrency and moved money for the networks, two North Korean delegation leaders based in Russia, six IT workers, and First Financial and Technical Development Center, a North Korean-controlled company in Russia that deploys IT workers. Treasury says the workers use fake documents, stolen identities and invented personas to obtain jobs at legitimate companies, that the North Korean government takes most of their wages, and that facilitators use cryptocurrency transfers, laundering methods and AI tools to move the proceeds. Treasury says the schemes have generated hundreds of millions of dollars for North Korea.



**WHAT THIS MEANS FOR FIRMS**

Firms should screen for the new designations and look for activity consistent with the scheme described by Treasury, such as accounts opened with inconsistent or stolen identity documents, unusual cryptocurrency conversions through intermediaries, and payments from overseas employers that do not fit the customer's profile. Firms that hire remote technology staff should apply robust identity and location checks.

ABOUT FINTRAIL

# 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

FINTRAIL
A COSEGIC COMPANY