FINTRAIL

Q3 2025

# REGCAP

A summary of the latest FinCrime regulatory news

www.fintrail.com

contact@fintrail.com

# Global



## Wolfberg Group statement on risk-based approach

The Wolfsberg Group has issued a statement outlining three key factors that FIs should keep in mind when designing and maintaining a risk-based financial crime programme:

1. Proportionality - the financial crime programme should be proportionate to the firm's business model as determined by its size, scale, footprint, customers and risk appetite.
2. Prioritisation - FIs should prioritise attention and resources to higher risk customers and activities, which might mean stopping and reducing other risk management measures in return.
3. Effectiveness - FIs should focus on responsive, forward-looking and dynamic approaches to financial crime risk management, rather than applying a one-size-fits all approach.



## Wolfsberg Group guidance on effective monitoring to detect suspicious activity

The Wolfsberg Group has issued a paper on effectiveness of monitoring suspicious activity, crucially noting that the Group does not believe ever-more SARs necessarily contribute to effectively fighting financial crime. Instead, the paper outlines how FIs should refocus efforts on detecting suspicious activity by for example:

- Reprioritise monitoring for suspicious activity through risk-based monitoring of customers, enhancing analytical capabilities, and pro-actively conducting holistic risk identification exercises across all customers, product and transactions
- Focusing on crystallised risk, by analysing the value of past SARs and incorporating information from SAR filings back into monitoring platforms.
- Enhancing data input, by incorporating other dynamic customer information such as device ID and IP addresses, in addition to static customer data.
- Utilising machine learning to boost models and improve detection capabilities.



## FATF publishes updated guidance on terrorist financing risks

The updated guidance takes into account emerging terrorist financing trends and insights from mutual evaluations over the last decade. Notably, the report covers in detail the current methods employed by terrorist organisations to raise and move funds through a number of sectors, including Fintechs. This includes:

- Mobile money, especially where registration of SIM cards is not enforced and peer-to-peer payments are possible.
- Online payments, appearing attractive for terrorists due to their low-cost and fast money transfer solutions.
- Social media platforms, used for their messaging with the use of QR codes for fast donations on the rise.



## The return of international sanctions on Iran

On September 28, 2025, all UN sanctions on Iran, previously lifted as part of the 2015 Joint Comprehensive Plan of Action, were reinstated. This happened due to the UK, France and Germany all triggering the so-called snapback mechanism contained in the JCPOA. The reimposed sanctions include:

- Comprehensive arms embargo and prohibitions on nuclear-related materials and technology.
- Asset freezes against individuals and entities in Iran.
- Restrictions on financial activities with Iran, including the establishment of correspondent banking relationships, and transactions - if these involve activities that could contribute to Iran's nuclear weapons programme.
- UN Member States are specifically called on to exercise vigilance over the activities of specific Iranian financial institutions, including Bank Melli, Bank Saderat and the Central Bank of Iran.

See the full list of reinstated UN sanctions measures here.

Further to the snapback of UN sanctions, on 29 September 2025 the EU also confirmed it would reimpose a number of its unilateral sanctions previously lifted, including a wider range of asset freezes on individuals, entities and several major Iranian banks. Read the EU statement here.

At the time of the JCPOA, the UK was part of the EU, and as of 29 September 2025 it remains to be seen what additional sanctions measures the UK will impose on Iran.

# Europe

## European Banking Authority publishes findings on ML/TF risks facing the EU's financial sector

The EBA notes that the rapid evolution of financial technologies and new financial products - and the growing interconnectedness of those products across sectors - have introduced unique new vulnerabilities. This includes:

1. Fintech innovation comes at the cost of compliance - the report notes that some fintechs may be prioritising customer acquisition over compliance.
2. Poor implementation of RegTech tools - while RegTech tools offer the potential for better compliance and reduction in manual errors, this can be hampered by inadequate in-house expertise, poor governance and insufficient oversight over these tools.
3. Fraud risks are escalating - new technologies continue to outpace the sector's defensive capabilities on fraud, including the use of AI for automation of schemes and making high-risk transactions harder to detect, as well as deep-fake technologies to evade CDD measures.
4. Sanctions risks are growing - the complexity of EU sanctions continues to challenge the financial sector, as new measures cannot be implemented by using standard sanctions screening tools alone.

## EBA report identifies opportunities for SupTech tools in supervision and enforcement

This EBA report takes stock of the current use of supervisory technology (SupTech) by EU regulators, and includes useful insight for industry as well. While the use of SupTech is still at an early stage, current use cases show it can strengthen AML/CFT supervision by improving data analysis capabilities, and helping regulators obtain comprehensive insights into firms' activities. The EBA concludes that the increasing adoption of SupTech tools - such as AI and synthetic data generation - signals a shift towards more efficient and data-driven supervision of financial crime.



**EBA fact sheet on use of AI highlights possible use cases in AML and fraud detection**

The European Banking Authority published a fact sheet on the rising application of AI in the EU banking and payments sector. The EBA has observed that 92% of EU banks are currently deploying AI in some form, including:

1. Delineating customer profiles according to their behaviour or grouping customers based on similarities.
2. Identification and verification of customers, where AI can improve the speed and efficiency of this process, as well as for enhanced risk profiling.
3. Real time monitoring of customers and transactions, including detection of patterns and anomalies related to ML/TF or fraud.

The fact sheet also identifies a number of challenges, including quality of data input with adequate data governance and human oversight.




FINTRAIL has published numerous popular guides and white papers on how firms can leverage AI effectively to strengthen their AML and fraud controls.

Discover more

# UK

## The new UK National Risk Assessment

### UK 2025 National Risk Assessment of Money Laundering and Terrorist Financing published

The UK published its new National Risk Assessment in July, following on from the previous NRA published in 2020. With a sharper focus on sector-specific threats, emerging typologies like crypto laundering and AI misuse, and the introduction of System Prioritisation, the direction of travel is clear: firms must take a more dynamic, threat-informed approach to risk management.

At FINTRAIL, we've reviewed the assessment in full, including the key changes firms need to be aware of, and the sectors most affected - for example, the ML/TF risks for EMIs/PSPs and cryptoassets have both increased since the last NRA was issued.

What the UK's 2025 National Risk Assessment Means for Financial Crime Compliance

**Read now**

The 2025 National Risk Assessment is a welcome step forward. For the first time, there is a sense that the UK is starting to take a genuinely threat- and risk-based approach to tackling financial crime. As our CEO, Robert Evans, put it:

> *"If we are honest with ourselves, to date the UK (and international) framework has been inherently ineffective and inefficient... So it is fantastic to see that this latest iteration is going to be complemented by annual typology and threat updates... This should mean that sectors covered by the MLRs can start to shift to a much more threat-informed approach to financial crime prevention in the UK"*

### System Priorities

Released alongside the NRA are the new System Priorities, agreed between the National Crime Agency, the Financial Conduct Authority, the Home Office and HM Treasury. The priorities are aligned to the NRA and designed to support firms in allocating resources to where they can have the most impact. The system priorities include:

- Sanctions evasion facilitated by UK-based professional enablers, particularly linked to Russia.
- Exploitation of money mules
- Fraud perpetrated by international organised crime groups with links to priority jurisdictions, including Ghana, Nigeria, India and Southeast Asia.
- Money laundering through UK corporate structures for OCGs with links to Albania, China, Russia and the UAE.

Read all 9 system priorities in full here.

## National Economic Crime Centre releases annual report outlining key economic crime threats

The report includes an overview of the NECC's activities and priorities, but also includes details of case studies and key threats identified by NECC. The annual report is therefore a good resource for firms to better understand the inherent threats they may be facing. This includes:

- Shutdown of a fraud platform thought to have exploited 170,000 victims across the UK.
- Operation Destabilise, the dismantling of a Russian-speaking network responsible for laundering funds for transactional criminal groups and helping Russian clients illegally move funds into the UK.
- Targeted operation targeting cash intensive businesses, including barbershops and vape shops.





## OFSI threat assessment for the cryptoasset sector and guidance on screening obligations for crypto transactions

The Office of Financial Sanctions Implementation has released another threat assessment, this time on the cryptoasset sector. The report highlights key sanctions threats in the sector, including:

- Almost certain that there is under-reporting of sanctions breaches within the crypto sector.
- It is highly likely that UK cryptoasset firms have been directly or indirectly exposed to Garantex, the designated exchange involved in Russian sanctions evasion, since its designation.
- Likely that UK cryptoasset firms are facilitating transfers to Iranian cryptoasset firms with links to designate persons.
- Likely that most non-compliance has occurred due to direct and indirect exposures, and delays in attribution.

Importantly, the report for the first time clarifies OFSI's expectations on determining indirect exposure and sanctions screening. The report states that "firms scan 3-5 [transaction] hops minimum in transaction history" to determine indirect exposure to sanctioned entities.

# Key UK regulatory updates

An overview of key fraud-related developments in the UK in the last quarter.

### FCA issues finalised PEP guidance

The FCA has published updated guidance on the treatment of PEP customers, following the outcomes of the 2024 PEP review. The guidance clarifies that "it is unlikely that a large number of UK customers should be treated as PEPs", and even where the person meets the definition of a domestic PEP the guidance and regulations requires that firms "recognise these customers' lower risk". The guidance sets out the measures that can be taken in lower risk situations.

### Proceeds of Crime threshold amount raised to £3,000

The threshold amount under the Proceeds of Crime Act (POCA), where firms must file a DAML to avoid committing an offence under POCA, has been raised from £1,000 to £3,000. Firms should ensure that internal reporting procedures are updated to reflect this new threshold.

### Money Laundering Regulations consultation response

The government published its consultation response on improving the effectiveness of the Money Laundering Regulations (MLRs), covering - among other things - how to make customer due diligence more proportionate and effective. Key themes include:

- Clarifying the term 'where necessary' for source of funds as part of ongoing monitoring
- Using digital identity for MLR identity verification checks
- Mandating EDD only where the relevant customer relationship involves a person in a Call for Action FATF country, not an Increased Monitoring List country. Note that broader requirements around assessing geographic risk - including the full FATF list - will remain for customer risk assessments.
- Amending EDD requirements to mandate EDD for "unusually complex" transactions as opposed to just complex transactions.

Read the full consultation response here and the new draft MLRs here (published September 2nd 2025).

# Key typologies and warnings

### FinCEN Notice on Financially Motivated Sextortion outlines common typologies

FinCEN has released a notice to help financial institutions detect and disrupt financially motivated sextortion - defined as perpetrators coercing victims to send sexually explicit material of themselves, and subsequently blackmailing the victim for money by threatening to release the material. The typologies should be adopted into firms' transaction monitoring rules and customer risk assessments. FinCEN notes that:

- While anyone can be targeted, boys between the ages of 14 and 17 are a particularly vulnerable and targeted group.
- The FBI saw a 59% increase in 2024 the number of reports received related to sextortion, compared to 2023.
- Perpetrators are increasingly using generative AI tools to create deepfake material of victims, from non-explicit content posted on a victim's social media pages.
- Transactions related to sextortion are often conducted using convertible virtual currency or prepaid cards.




### Red Alert on Shadow Fleet sanctions evasion

The UK National Crime Agency released a Red Alert on sanctions evasion by Russia's shadow fleet. The notice describes how these networks operate: one side actively trades Russian oil through a network of front companies, with another side of the network set up to deal with banks and insurers in Western countries. The alert also includes key red flag indicators that firms should be aware of - including transfers between obscure companies, companies operating in jurisdictions where shadow fleet entities are based, with a limited presence only and with limited previous trading history.



### FinCEN analysis of Chinese money laundering networks in the US

FinCEN released a notice outlining threat patterns identified by analysing 137,153 BSA reports associated with suspected Chinese money laundering network (CMLN) activity. The trends identified include:

- CMLN's rely on US-based Chinese nationals to deposit cash into the financial system.
- US-based CMLNs recruit buyers (so-called 'daigou') to purchase high-value electronics and luxury goods for export out of the US, in order to launder illicit proceeds.
- CMLN's are potentially using adult daycare centers, in particular in New York, and real estate purchases to further launder funds.
- CMLN's may also use Chinese students to gain access to many bank accounts to place illicit proceeds into the financial system.

## FinCEN analysis of Chinese money laundering networks in the US

FinCEN released a notice outlining threat patterns identified by analysing 137,153 BSA reports associated with suspected Chinese money laundering network (CMLN) activity. The trends identified include:

- CMLN's rely on US-based Chinese nationals to deposit cash into the financial system.
- US-based CMLNs recruit buyers (so-called 'daigou') to purchase high-value electronics and luxury goods for export out of the US, in order to launder illicit proceeds.
- CMLN's are potentially using adult daycare centers, in particular in New York, and real estate purchases to

## UK and US take joint action to target Russian crypto sanctions evasion networks

In August, both the UK and the US took similar actions to target a key cryptocurrency exchange used by Russia to evade sanctions.

- Both countries targeted Grinex, an exchange providing infrastructure for A7A5 - a token specifically designed to evade Western sanctions against Russia, and other firms involved in creating the token.
- The US press release notes that Grinex is the successor to Garantex - the Russian cryptocurrency exchange previously designated for facilitating hundreds of millions of illicit funds for ransomware groups.

In September, Transparency International also published an in-depth investigation into how Garantex successors - including Grinex - have allowed the Garantex ecosystem to survive after designation. Any firms with crypto exposure should understand the methods used by the networks and be aware of the footprints in Europe of the network.



## FinCEN Notice on Financially Motivated Sextortion outlines common typologies

FinCEN has released a notice to help financial institutions detect and disrupt financially motivated sextortion - defined as perpetrators coercing victims to send sexually explicit material of themselves, and subsequently blackmailing the victim for money by threatening to release the material. The typologies should be adopted into firms' transaction monitoring rules and customer risk assessments. FinCEN notes that:

- While anyone can be targeted, boys between the ages of 14 and 17 are a particularly vulnerable and targeted group.
- The FBI saw a 59% increase in 2024 the number of reports received related to sextortion, compared to 2023.
- Perpetrators are increasingly using generative AI tools to create deepfake material of victims, from non-explicit content posted on a victim's social media pages.
- Transactions related to sextortion are often conducted using convertible virtual currency or prepaid cards.

# Stories from around the world

**FinCEN encourages more cross-border sharing of information on financial crime**
FinCEN has published a notice to encourage financial institutions to share information on financial crime, and provides guidance on what firms should consider when they share information across borders:

- Firms should consider their risk profile and their relationship with the foreign financial institution.
- While the BSA prohibits the disclosure of a SAR ('tipping off') it "does not prohibit sharing the underlying facts, transactions and documents upon which a SAR is based" including with foreign financial institutions.

**Canada's National AML/CFT Risk Assessment notes that drug trafficking, fraud and tax crimes remains highest money laundering threats**
Canada has released its 2025 National Risk Assessment on AML/CFT, which identifies that drug trafficking, fraud and tax crimes remain the highest money laundering threats in the country, and particular identifies money service businesses, crypto assets and domestic banks as particularly vulnerable, as they are accessible to individuals both within Canada and abroad, and can facilitate rapid movement of funds. For terrorist financing, the risk assessment notes that most attacks are perpetrated by ideologically motivated lone actors, requiring low volume and low value. The report is a useful tool for any firms with a Canadian license or with significant exposure to Canada.

**BIS strengthens export controls through new 50% ownership criteria**
The US Department of Commerce has issued a new rule that creates a 50% ownership rule, similar to the 50% OFAC rule used for blocking sanctions. The rule means that any entity that is at least 50% owned by one or more entities on the BIS Entity List or the Military End-User List will itself be subject to those same export control restrictions. Previously, entities not specifically named themselves on the list were excluded. In addition, BIS notes that minority ownership should also be a red flag that triggers additional due diligence.

Firms should ensure that their screening list providers are making the appropriate updates to expand BIS-related lists to cover entities owned 50% or more by any of the entities on the Entity List or the Military End-User List.

# Enforcement actions

### France: Banque Delubac

The ACPR fined Banque Delubac €600,000 for multiple financial crime compliance failures, including not collecting sufficient data on directors and beneficial owners of their customers. In addition, the bank did not screen transactions valued below €1,000 between 2020 - 2022.

Lesson: Be sure you understand regulatory expectations in full and where a risk-based approach cannot be used - France has clear regulatory requirements for conducting payment screening.



### Singapore: 9 Financial Institutions fined for AML-related breaches

The Monetary Authority of Singapore has fined 9 banks in a composite penalty for various AML failures, discovered during MAS supervisory visits from 2023 - 2025. This includes:

- Customer risk assessment: 5 banks failed to implement adequate processes for rating the money laundering risks of their customers, which affected the banks' ability to apply appropriate controls.
- Source of wealth: All 9 banks did not detect or adequately follow up on red flags in customers' source of wealth documentation in some cases where there were signs of increased risk of money laundering.
- Transaction monitoring: 8 banks failed to adequately review unusually large transactions inconsistent with customer profiles that were flagged as suspicious by their own system.
- Post-STR follow up: 2 banks failed to apply enhanced monitoring on customers the banks had filed STRs on.

Lesson: Many of these failings could have been prevented through ongoing quality assurance and audit of the banks' financial crime processes, for example the use of dip testing and four eye review and escalation of high risk cases.



## US - OFAC: Interactive Brokers LLC

OFAC fined Interactive Brokers $11.8 million for multiple sanctions control failures, including failures around IP and geoblocking controls:

- Providing services to ~200 customers in sanctioned jurisdictions, including Iran, Cuba, Syria and Crimea. While the customers' KYC information stated their residence was elsewhere, subsequent IP data and search engine results revealed the customers were in fact located in sanctioned jurisdictions when they made transactions.
- While the firm did have IP geo blocking controls in place, this had some deficiencies.

Interactive Brokers were further fined for facilitating transfers to sanctioned Russian banks, providing new investment to Russia, and other violations.

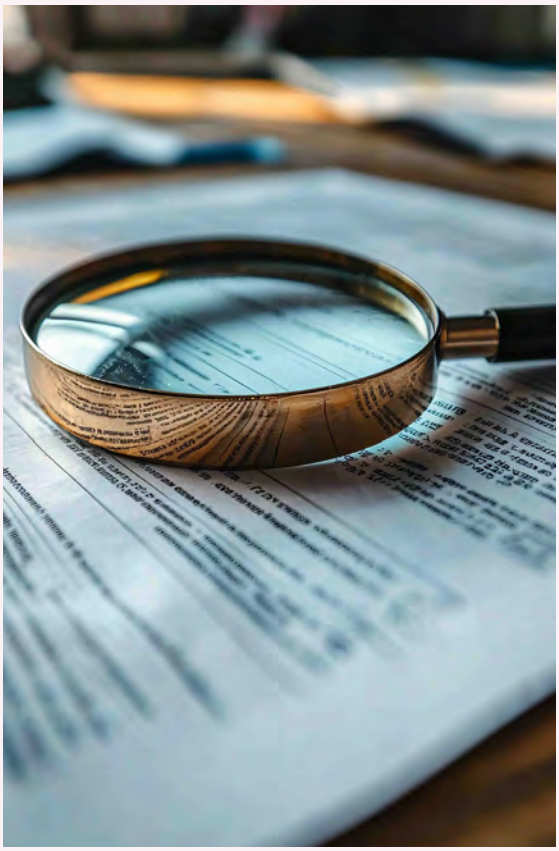
Lesson: This enforcement action shows the importance of using all information available on customer location - including their declared address, as well as IP address information during the course of the business relationships and other geolocation data.



## Netherlands: Bunq

De Nederlansche Bank (DNB) has fined Bunq €2.6 million for deficiencies in how the firm conducts its ongoing monitoring of high risk customers. Specifically, the fine notes how the firm was deficient in following up on transaction monitoring alerts involving high risk customers, meaning there was a risk that unusual transactions were either not detected or reported or not detected and reported in time. Bunq had previously been asked to improve controls, but the DNB found that the firm had not made sufficient progress.

Lesson: Firms must ensure that customers flagged as high risk for money laundering or terrorist financing are subject to enhanced monitoring throughout the customer relationships, and that the firm has clear procedures for escalating and reporting suspicious transactions involving these customers in particular.



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.