FINTRAIL

Q2 2025

REGCAP

A summary of the latest FinCrime regulatory news

www.fintrail.com

contact@fintrail.com

Global

Financial Action Task Force plenary

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

Added to FATF Greylist	Removed from FATF Greylist
Bolivia	Croatia
British Virgin Islands	Mali
	Tanzania

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

1. Changes to Recommendation 16 of the FATF Standards may reduce the need for RFIs

The changes streamlines the requirements for information that must be included in peer-to-peer cross-border payments (name, address and date of birth), potentially making it easier in future to identify who is sending and receiving money and aiding screening and transaction monitoring efforts. For financial institutions it may reduce the need for sending Requests for Information in future.

The standards also introduce requirements to introduce tools to protect against fraud, such as verification of recipient bank account information. The changes come into effect by the end of 2030.

2. Updated guidance on Financial Inclusion provides examples of simplified due diligence

This new guidance provides practical examples of how simplified due diligence measures can be applied in lower risk situations to support financial inclusion. Specifically this includes reduction of identification requirements in certain situations, alternative means of identification where standard ID cannot be provided, verification after the establishment of a business relationship and tailored ID&V based on the customer's risk profile.

3. Report on sanctions evasion schemes highlights the role of Russia as a strategic partner to North Korea

The report provides detailed analysis of the key techniques used by particularly North Korea and Iran to evade financial sanctions related to proliferation The report highlights four major typologies:

1. Enlistment of intermediaries to evade sanctions.
2. Obscuring beneficial ownership to access the financial system
3. Using virtual assets and other technologies
4. Exploiting the maritime and shipping sectors.

Crucially, the report highlights the role of Russia as a key strategic partner for North Korea, and the increasing proliferation financing threat stemming from Russia. While many of the typologies in the report are well-known, the case studies in the report are real world examples provided by member states and provide useful illustrations of sanctions evasion schemes in practice.

4. The 6th Targeted Update Report on countries' implementation of FATF Standards in relation to Virtual Assets notes rising use of stable coins by illicit actors.

The report notes that 73% of countries (excluding those prohibiting crypto) have now implemented the Travel Rule, but notes that many countries are facing difficulties identifying natural or legal persons that conduct VASP activities. The report highlights key risks of virtual assets being used by criminals and organised crime groups for scams, terrorist financing and illegal gambling. It also notes that the use of stable coins by illicit actors has risen in the last year.

UK

FCA sets out its financial crime priorities for 2025-2026
The Financial Conduct Authority published its annual work programme for 2025-2026. Of note for financial crime, the FCA will continue with proactive assessments of anti-money laundering systems and controls for firms they deem higher risk, including engaging firms to strengthen their sanctions systems.

The FCA also announced two new streams of work:
1. Building a data-led detection capability, which will enable the FCA to increase identification of financial crime in regulated firms.
2. Increased collaboration with partners to tackle money laundering connected to serious organised crime.

Firms should note that the FCA is actively working with other regulators and law enforcement bodies both domestically and internationally to share data and identify financial crime.

OFSI guides provides insight into sanctions risks of legal services industry, property services and the art/high value dealers
The **Office of Financial Sanctions Implementation** has published three additional guides outlining the key risks and threats to specific sectors. These all focus on Russia sanctions threats:

- Legal services: The report highlights the risk of complex corporate structures, including trusts, linked to Russian designated persons among other threats that the legal sector should stay alert to.
- Property and related services: The report noted it was almost certain that UK property firms have under-reported breaches of sanctions, and that sanctioned persons have breached sanctions by making transactions for their UK properties without a license.
- Art Market Participants and High Value Dealers: The report notes the likelihood that Russian designated persons have dealt in high value goods in the UK.

All three include red flags for the sectors to be aware of. While the reports are targeted towards the sectors in question, any financial institution who facilitates payments for art and high value dealers, property services or the legal profession would benefit from reading the reports to understand the sanctions risk exposure from these industries.





Cross-government review of UK sanctions identifies need to increase the deterrent effect of sanctions enforcement

The **UK Government** released a cross-government review of the UK's implementation and enforcement of sanctions. Crucially for financial firms is the review conclusion that "to give sanctions bite, there must be clear consequences for offenders" and highlights the need to have a "balance between civil penalties, criminal prosecutions and other disruptions".

The review set out a number of priorities for the year 2025-2026, including:

1. Creating additional guidance for, and increasing engagement with, sectors less familiar with sanctions compliance.
2. Regular publication of sanctions enforcement action and disruptions to take advantage of "teachable moments".
3. Develop an accelerated civil penalty process for certain financial sanctions breaches, to free up resources to focus on more complex, serious and deliberate offences.

Based on the actions and priorities set out in this review, in 2025-2026 we can expect the number of sanctions enforcement actions to increase.

Updated FCA enforcement guide sets out criteria for announcing investigations into regulated firms

On June 3, the **Financial Conduct Authority** released its final version of the updated enforcement guide. After feedback there will no longer proceed with the public interest framework originally proposed (also referred to as the "name and shame" approach). The guide identified three situations where there was broad support for increased transparency in ongoing investigations:

Where an announcement will warn consumers or investors or help the investigation.

Where the fact of the investigation has been made public by the subject or a regulatory body or government.

Anonymised announcements, not naming or identifying the subject of the investigation, where it would be helpful to educate people on the types of misconduct the FCA is investigating.

New cryptoasset regulation announced

The **UK Government** announced on 29 April 2025 draft legislation for regulating cryptoassets. Under these rules, crypto exchanges, dealers and agents will be brought into the regulatory framework, and crypto firms in the UK will be subject to new standards on consumer protection. Practically speaking, this extends current UK regulatory frameworks for financial services to firms that deal, operate platforms or arrange transactions in qualifying cryptoassets, and will need to be authorised and regulated by the FCA.

UK announces new rules to guard against debanking

The **UK Government** announced on 28 April new rules that will require banks to give customers 90 days' notice before closing accounts or terminating a payment service and provide a clear explanation. This will provide customers enough time to challenge decisions, and will prevent banks from closing accounts without reason. The government notes that there will be certain exceptions to this rule, for example to comply with obligations under financial crime law, including the provision not to tip off customers.





Spotlight: What the Fraud

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

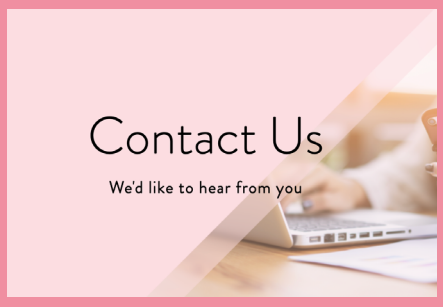
APP fraud has fallen, but other types of fraud have increased

UK Finance released its Annual Fraud Report 2025, which shows that losses stemming from APP fraud decreased in 2023-2024 (£459.7 in 2023 to £450.7 million in 2024) with the overall number of APP fraud cases also declining (from 232,427 cases in 2023 to 185,733 cases in 2024). Investment scams continue to be a big driver of APP fraud losses, accounting for nearly a third of APP losses. However, at the same time, other types of fraud are increasing, including remote purchase card fraud (with cases up 22%). The report notes that "discussions with industry point to an increase in the compromise of one-time passcodes (OTPs), which are used to register digital wallets and compromise cards".

PSR report notes no rise in APP fraud rates and better industry cooperation on fraud reimbursement

The **Payment Systems Regulator** released a report on 15 May 2025 highlighting progress made since APP fraud reimbursement rules came into force in October 2024. The report highlights:

- Reimbursement Rates - Reimbursement rates for victims are high and vulnerable customers are better protected with 86% of APP money lost returned to victims in the first 3 months of new rules being live.
- Cooperation - Early data shows a more level playing field amongst the industry, with most claims (86%) being reported by the sending firm to the receiving firm within 2 hours of the consumer raising the claim.
- Fraud rates - despite industry concerns that APP fraud claims may increase, this has not been the case. The data suggests that the volume of APP scam claims submitted by consumers was lower relative to a similar period in 2023.
- Customer caution - Only 2% of total claims were rejected due to the consumer caution exception with no significant shift in consumer behaviour identified.



Want to know more about how FINTRIAL has supported firms in managing their anti-fraud framework?

Read case study | Contact us

Europe

Updates to the EU High Risk Country List mismatches the FATF greylist

The **European Union** has updated its list of third countries with strategic deficiencies in their regime on anti-money laundering and countering terrorist financing. While the EU's list takes into account the FATF's findings on countries, the lists are not aligned. The below table shows the current alignment between the FATF list and the EU list, following both the updates made by the EU and the FATF plenary in June. Financial institutions operating in the EU should therefore take into consideration both lists, when determining their own internal list of high risk countries.



Country	FATF	European Commission
Afghanistan	No	Yes
Algeria	Yes	Added
Angola	Yes	Added
Bolivia	Added	No
Barbados	No	Removed
Bulgaria	Yes	No
Burkina Faso	Yes	Yes
Cameroon	Yes	Yes
Côte d'Ivoire	Yes	Added
Croatia	Removed	No
Democratic Republic of Congo	Yes	Yes
Gibralta	No	Removed
Haiti	Yes	Yes
Jamaica	No	Removed
Kenya	Yes	Added
Laos	Yes	Added
Lebanon	Yes	Added
Mali	Removed	No
Monaco	Yes	Added
Mozambique	Yes	Yes
Myanmar	No	Yes
Namibia	Yes	Added
Nepal	Yes	Added
Nigeria	Yes	Yes
Panama	No	Removed
Philipines	No	Removed
Senegal	No	Removed
South Africa	Yes	Yes
South Sudan	Yes	Yes
Syria	Yes	Yes
Tanzania	Removed	Yes
Trinidad and Tobago	No	Yes
UAE	No	Removed
Uganda	No	Removed
Vanuatu	No	Yes
Venezuela	Yes	Added
Vietnam	Yes	Yes
British Virgin Islands	Added	No
Yemen	Yes	Yes

European Union Terrorist Situation and Trend Report 2025 points out risk of "digital hawala" and generative AI

Europol has published its annual report on terrorist attacks, arrests and convictions in EU member states. Of relevance to financial firms is the continued use of cryptocurrencies in so-called "digital hawala" - the digital adaptation of the traditional hawala system - for terrorist financing purposes. The report also highlights the use of generative AI to create and disseminate terrorist propaganda and hate speech at "unprecedented levels".





European Banking Authority annual report highlights key outputs for 2024

The **European Banking Authority (EBA)** published its annual report for 2024 outlining its key achievements and activities, including on AML/CFT. This includes guidelines on the travel rule for crypto assets, guidelines on the implementation of EU sanctions, consultation on the draft standards for crypto asset service providers to appoint a central point of contact for AML/CFT, and more. The report also notes that the EBA will continue to be responsible for AML/CFT matters until 31 December 2025, after which AMLA - the new EU anti-money laundering authority - will take over much of this work.





EBA extends technical standards on central contact points to crypto-asset service providers

The EBA has released draft technical standards on the criteria for the appointment of central contact points for AML/CFT for firms in EU member states. As is the case for EMIs and PSPs, CASPs can provide services in other Member States through establishments other than branches. While the technical standards are already in place for PSPs and EMIs for when they must appoint a central contact point in certain member states they are active in (even if they are not regulated there). These updated technical standards extends that scope to crypto asset service providers.





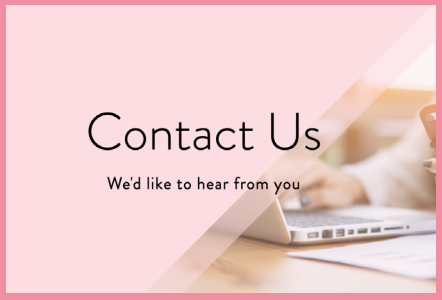
Spotlight: Syria

Syria has been subject to comprehensive international sanctions since 2011. In the last quarter however, following the fall of the Assad regime, these sanctions imposed by the US, EU and UK have gradually been lifted in order to encourage re-engagement with the new Syrian government, and allow certain financial and trade flows into Syria.

This includes:

- **The EU** adopted a series of legal instruments on May 28 2025 which lifted most sanctions targeting Syria as a country, including restrictions on relationships with Syrian banks and the delisting of several Syrian banks (including the Central Bank), while maintaining sanctions related to the former Assad regime and those imposed on other grounds.
- **The UK** adopted the Syria (Sanctions) (EU Exit) (Amendment) Regulations 2025 on April 24, revoking measures contained in the Syria sanctions regime targeting the finance, energy, trade and transport sectors. This again includes restrictions on dealing with most Syrian banks, including the Central Bank.
- **The US**, on June 30th 2025, removed a number of Executive Orders that previously placed comprehensive sanctions on Syria, including the delisting of over 500 individuals and entities in Syria, including banks.

However, as some sanctions are removed, key sanctions restrictions remain in place and other financial crime risks relating to Syria remain. In the last quarter, FINTRAIL helped a cross-border payments firm navigate the complex nature of sanctions lifting - and the business opportunity this presents - with financial crime, terrorist financing and other risks still present in Syria. We developed bespoke due diligence steps unique to the firm's products and customers, to help mitigate financial crime risks when dealing with Syria.



Get in touch with the team, if you are thinking of payment services to high-risk jurisdictions including Syria.

Contact us

Highlights from around the world

United States: FinCEN issues advisory on Iranian oil smuggling and shadow banking
On June 6 2025, the **Financial Crimes Enforcement Network** (FinCEN), released an advisory to financial institutions to help them identify and report suspicious activity connected to Iranian illicit financial activity, including oil smuggling, "shadow banking," and weapons procurement. The report highlights that Hong Kong-based companies that bank with China-based financial institutions using non-resident accounts and UAE-based general trading companies registered in commercial free trade zones are commonly used as front companies by Iranian actors. Any firms with clients who fit this profile should stay alert to this typology.

Australia: FinTech and DeFi specific sanctions guidance
The **Australian Sanctions Office** released guidance specifically directed at Fintech and DeFi companies. The guide notes sanctions risks across customer, jurisdiction, transaction and product/service risks, and is therefore a useful starting point for conducting sanctions risk assessments, regardless of the jurisdiction your firm is in. For example, the guidance specifically states that it is expected forms will implement robust IP and address checks to avoid providing services to sanctioned regions.

Germany: BaFin's annual report highlights actions taken against senior managers
On June 6 2025, **BaFin** released its annual report for 2024, and noted that due to persistent violations of money laundering regulations, it is increasingly taking measures against senior managers. BaFIn notes that "senior managers are responsible for ensuring a proper business organisation, which includes measures to prevent money laundering and terrorist financing".

The report also notes that **BaFin** has further intensified its preventative supervision on financial crime through routine and ad hoc special audits in the banking and non-banking sectors, increasingly focused on high-risk products and business models.

France: AML/CFT threat assessment
Tracfin released its AML/CFT Threat Assessment for 2023-2024, highlighting key observed money laundering and terrorist typologies and case studies across various sectors, including art dealers, crypto assets, NFTs, gambling, real estate, social media and more. The report is a key resource for firms to understand how various financial crime typologies are carried out in practice, and includes lists of warning signs/red flags for firms to stay alert to. It could also be a useful reference for any firms wishing to increase their understanding of inherent financial crime risks they are exposed to through different client sectors.

UAE: National Risk Assessment identified fraud and drug trafficking as significant money laundering threats in the UAE

The UAE released its 2024 National Risk Assessment on 24 April 2025. Overall, it concludes the money laundering threat to be medium-high, with fraud and drug trafficking being the most significant threats. The risk assessment further notes that the UAE's banking sector remains attractive to criminals due to its size and extensive cross-border network.

For terrorist financing, the risk assessment assesses the residual risk as medium high. Despite stringent regulatory measures, the use of unregulated money transfer services and the manipulation of the trade sector for TF purposes persist. Money or Value Transfer Services (MVTS) is frequently exploited by various organisations and is identified as the most utilised financial channel for terrorist financing, followed by the hawala sector.

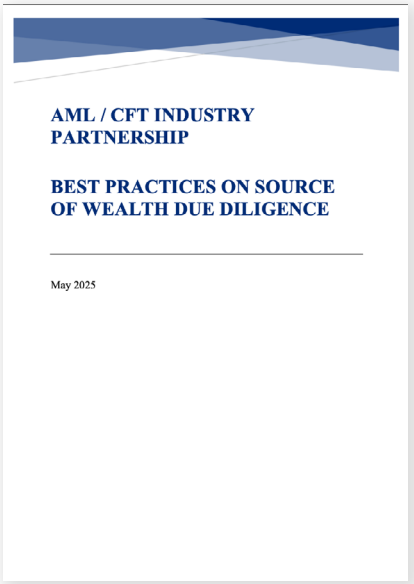
Any firm who operates in the UAE, or has significant exposure to the UAE, should read the risk assessment in full to ensure their own risk assessment adequately reflects the risks identified by the National Risk Assessment.



Singapore: Guidance on Source of Wealth Due Diligence

The **AML/CFT Industry Partnership (ACIP)**, a public private partnership between regulators and industry in Singapore, has released a __ setting out best practice for establishing a customer's source of wealth. The guidance covers how financial institutions may adopt a tiered approach to source of wealth due diligence to determine which customers should be subject to additional SoW corroboration.





Spotlight: Cyber-enabled financial crime

A number of reports this quarter provide key insights into cyber-enabled financial crime.

The **Global Initiative Against Transnational Organized Crime** released a report on cyber scam operations in Southeast Asia, and provides details into how cyber scams - including romance scams, investment scams, crypto fraud and sextortion - are operated and generate tens of billions of dollars annually.



Europol has published its 2025 Internet Organised Crime Threat Assessment, which provides insight into cybercrime - from phishing to phone scams - and how stolen data has become weaponised by cybercriminals to enable these crimes.



The **FBI** released its annual report on Internet Crime. The report notes that the top three cyber crimes, by number of complaints reported by victims in 2024, were phishing/ spoofing, extortion, and personal data breaches.





Key enforcement actions: Lessons learned

UK: £5000 for failing to respond to RFI from OFSI

The UK's **Office of Financial Sanctions Implementation (OFSI)** fined Svarog Shipping £5000 for failing to respond to a Request for Information sent by OFSI by the stated deadline, despite OFSI sending reminders to the firm. OFSI only received a response after it contacted Svarog's auditors, but no reasonable excuse for missing the statutory deadline was provided.

OFSI notes in an accompanying blog post that it "takes a dim view of firms who delay or fail to respond" and that these delays, if repeated by other firms, "could seriously undermine OFSI's effectiveness and efficiency".

The key lesson for firms is to engage proactively with any RFIs issued by law enforcement or regulators, and have processes in place to identify incoming RFIs and formulate a response by the deadline.

Singapore: Composition penalties against five payment institutions

The **Monetary Authority of Singapore** has imposed composition penalties against five Major Payment Institutions (MPIs) who all provide cross-border payment services, for various breaches of AML/CFT requirements. The breaches include:

- Failure to verify the identity of customers using reliable, independent source data.
- Failure to obtain residential addresses of customers.
- Failure to identify beneficial owners.
- Failure to screen customers and connected parties against relevant ML/TF sources when establishing business relations.
- Failure to include relevant wire transfer information in the message or payment instructions for cross-border wire transfers.

The MAS notes that common to all five cases "MAS expects the senior management of financial institutions to play an active role to oversee the implementation of adequate AML/CFT controls". The key lesson learned for payment institutions offering cross-border services is the need to identify and verify customers and beneficial owners, and include adequate originator and beneficiary information in payment instructions.



UAE: Virtual Asset firm fined $8.85 million, including fines for senior management

The **Abu Dhabi Financial Services Regulatory Authority** fined the Havyn Group - a group of entities providing virtual asset services in Abu Dhabi - a total of $8.85 million for various money laundering-related deficiencies. Specifically:

- Firms did not have systems and controls in place to recognise and record all of its client relationships, thus breaching Abu Dhabi anti-money laundering requirements.
- Havyn facilitated the conversion of virtual assets to fiat currency (and vice versa) through an unlicensed entity.
- The penalty identifies specific senior personnel who were centrally involved in the misconduct, and ultimately held responsible. The senior official in question was fined $750,000 personally.
- The firm provided false and misleading information to the FSRA in response to requests for information.

The key lesson for firms - in particular in the virtual assets industry - is to ensure proper registration and licensing of all activities, including the ability to onboard and record customers in line with regulatory requirements.



UK: Art dealer jailed for failing to report suspicious transactions related to terrorist financing

An art dealer was sentenced for 2 years and 6 months for failing to declare art he knowingly sold to a suspected Hezbollah financier. This is the first prosecution - and conviction - for failing to make a disclosure related to suspicious transactions under the Terrorism Act 2000. The art dealer, Oghenochuko Ojiri, sold art to a customer who was sanctioned in 2019 by the US for being a donor to Hezbollah (but was not yet sanctioned in the UK). The evidence seized from his phone showed he had researched who Mr Ahmad was and knew he had been sanctioned by the US. A colleague had even messaged to warn him against doing business with Mr Ahmad.



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.