

WEEK OF 22-28 SEPTEMBER 2026

Financial Crime Weekly Digest

Global enforcement actions, regulatory moves & intelligence from the world of AML & financial crime.

STORY OF THE WEEK

The Central Bank of the UAE bars every UAE branch of Bank Melli Iran from transactions to and from Iran, trade finance included

ENFORCEMENT

A travel-agency front and over \$20m through 57 accounts · a sextortion launderer pleads guilty · fake IDs couriered from the UAE

REGULATORY

FATF publishes Türkiye's mutual evaluation · the FCA finds mule money usually cashes out by the fifth account

STORY OF THE WEEK · UAE / IRAN

The CBUAE Bars Bank Melli Iran's UAE Branches From Iran Transactions

ALL BRANCHES

of Bank Melli Iran operating in the UAE, prohibited from any financial transactions to and from Iran, including trade finance and fund transfers

On **23 September** the Central Bank of the UAE announced “the imposition of strict enforcement measures against the branches of Bank Melli Iran operating in the UAE”, in accordance with **Article (168-1-C) of Federal Decree-Law No. (6) of 2025** regarding the Central Bank, Regulation of Financial Institutions and Activities, and Insurance Business. The CBUAE says the measures result from violations related to **non-compliance with the regulations, laws and supervisory decisions in force in the UAE**, including requirements under the legislation on combating **money laundering, the financing of terrorism and proliferation financing**. Based on the results of its examinations, and under the powers granted to the CBUAE Governor, it has been decided to **prohibit all branches of Bank Melli Iran operating in the UAE from conducting any financial transactions to and from Iran, including trade finance and fund transfers**.

Read the release for what it does not say. It states **no fine or monetary amount**, gives **no number of branches**, and does not itemise the violations beyond the categories above; we have added none. The headline speaks of “strict sanctions”, but the body describes **enforcement measures under the central bank law** following examinations — a supervisory action, not a listing. Trade finance is not new territory for the CBUAE: its own proliferation-finance guidance already tells institutions to be aware of the potential vulnerabilities of **Iran transactions associated with trade finance**, and to put controls in place.

- Legal basis: Article (168-1-C) of Federal Decree-Law No. (6) of 2025 · announced 23 Sept 2026
- Grounds: non-compliance including AML, CFT and proliferation-financing requirements, found on examination
- Measure: no financial transactions to and from Iran, including trade finance and fund transfers
- No fine, amount or branch count is given in the release

WHY IT MATTERS FOR COMPLIANCE TEAMS

This is a corridor closed by a supervisor, not a name added to a list, so it will not arrive through a screening file. **UAE banks and exchange houses that deal with Bank Melli Iran's UAE branches — as correspondents, on trade documents, or as counterparties on transfers — should check which of those flows touch Iran, because the branches are now prohibited from conducting them.** And keep the file note exact: the CBUAE cites examination findings and the central bank law, and names AML, CFT and proliferation-financing obligations. It gives no fine, and nothing in the release should be written up as one.

ENFORCEMENT ACTIONS

Law Enforcement Strikes This Week

US DEPARTMENT OF JUSTICE · UNITED STATES / CUBA

JURY CONVICTION

A Travel Agency as a Front, and Over \$20 Million Through 57 Accounts

On **25 September** the Justice Department announced that a federal jury in the Middle District of Florida had convicted **Lazaro Alain Cabrera-Rodriguez**, 28, of Hialeah, of **conspiracy to commit alien smuggling for financial gain, conspiracy to commit international money laundering, and conspiracy to commit money laundering concealment**. According to court documents and trial evidence, he conspired to operate an alien smuggling organisation that encouraged thousands of Cuban aliens to enter the US through the southern border, charging **between \$1,500 and \$40,000**, and filed hundreds of fraudulent ESTA applications using fake addresses. **Financial records show that over \$20 million passed through upwards of 57 bank accounts** controlled by the defendant and his co-conspirators. Assistant Attorney General Duva described the travel agency as providing “a veneer of legitimacy to evade detection”. Sentencing is set for **17 December**; the **maximum** is 20 years.

US DEPARTMENT OF JUSTICE · UNITED STATES / NIGERIA

GUILTY PLEA

Sextortion and Romance-Scam Proceeds, Laundered Through P2P Apps and Crypto

On **22 September** the Justice Department announced that **Olamide Shanu**, 35, a Nigerian national extradited from Nigeria, had pleaded guilty the previous day in the District of Idaho to **conspiracy to commit money laundering**. The department says the schemes defrauded **approximately 150 American victims**, caused millions of dollars in losses, and earned Shanu **more than \$2,500,000**. The co-conspirators ran sextortion, typically against male victims, and romance scams using fake identities on social media. The laundering route is stated plainly: **proceeds were laundered using peer-to-peer payment applications and several cryptocurrency wallet addresses before being transferred to the co-conspirators in Nigeria**. This is a **guilty plea, not a trial verdict**; sentencing is scheduled for 15 December and the **maximum** penalty is 20 years.

EUROPOL · AUSTRIA / ITALY / SPAIN / UK / UAE

6 ARRESTS

Fake IDs Couriered From the UAE, and Phone Shops to Launder the Profits

Europol announced on **23 September** that it had supported a migrant smuggling investigation involving authorities from **17 countries**, against a network **also engaged in document fraud and money laundering**. The **action day on 22 September** in Austria, Italy, Spain and the UK led to **six arrests, 10 house searches** and seizures including ID documents and **a large amount of cash**. A Vienna-based cell is connected with setting up a network of services, **primarily mobile phone shops, to allegedly launder criminal profits**. A Spain-based cell allegedly facilitated the distribution of **over 1,000 fake IDs, sent via couriers from the United Arab Emirates** to the EU, the Americas and the Caribbean. Investigative leads suggest the wider network generated **more than EUR 2 million** in illegal proceeds. Europol's support covered both the migrant smuggling and the **financial investigations**. The conduct is alleged; no conviction has been announced.

REGULATORY DEVELOPMENTS

Regulatory Moves Reshaping the Compliance Landscape

GLOBAL / TÜRKİYE

FATF Publishes Türkiye's Mutual Evaluation — Enhanced Follow-Up

On **23 September** the FATF published its mutual evaluation of **Türkiye**, which assessed the effectiveness of its AML/CFT/CPF measures and its compliance with the FATF Recommendations **at the time of its on-site visit in November 2025**. The headline is balanced: Türkiye has strengthened its defences, including through better use of financial intelligence and international co-operation, but should further prioritise money laundering investigations and prosecutions for certain high-risk predicate offences and strengthen its capacity to **identify, trace and recover criminal assets located abroad**. Based on its effectiveness and technical compliance ratings, **Türkiye is placed in enhanced follow-up**. The findings a correspondent or onboarding team will recognise: among financial institutions and VASPs, **Politically Exposed Person identification and monitoring is only partially effective**, and shortcomings continue to be identified in suspicious transaction reporting; understanding of TF risk is more limited outside banking; and understanding of ML/TF risk is less developed for **foreign-created legal persons** with links to Türkiye, with **major improvements needed** to keep basic and beneficial ownership information accurate and up to date. The FATF says the FIU, MASAK, plays a central and effective role, with direct access to more than 300 databases. The report records **over 10,000 prosecutions** of ML and predicate offences, but also a backlog of pending prosecutions (7,248 cases) and convictions (6,085). Of the 40 Recommendations, only R.7 (proliferation TFS) and R.8 (non-profit organisations) are rated partially compliant.

UNITED KINGDOM

The FCA on Money Mules: Cash-Out Comes Between the Second and Fifth Account

On **23 September** the FCA published findings from a multi-firm review of money mule activity. An FCA survey of **35 retail banks, building societies, challenger banks, payment institutions and e-money institutions** found that **238,396 suspected mules had their accounts closed in 2025**, up from 184,935 in 2023 and 233,269 in 2024. The FCA is careful about what that means: the increase could reflect broader customer growth alongside better identification, **rather than necessarily meaning mules make up a higher proportion** of firms' business. Closures were highest among customers aged 26 to 39 (91,073); the sharpest increase was among 40- to 49-year-olds (37,274 in 2025, up from 25,760 in 2024). The operational finding is the one to act on: criminals moved fraudulent funds through multiple accounts, **usually cashing out between the second and fifth account**, by which point payments are harder to detect and trace. **Card payments were the most common cash-out method**, often many low-value transactions or higher-value payments to local businesses that can resemble legitimate spending. Some accounts had been used repeatedly for mule activity, and for fraud, before closure, which the FCA reads as **established criminal infrastructure** rather than isolated incidents. A public/private cell set up in 2025 with 22 regulated firms looked at 140 cases covering 7 types of fraud. For scale, the FCA cites the National Crime Agency's estimate that **more than £100bn** is laundered through the UK or UK corporate structures each year.

ON OUR RADAR

Watch This Space

CRYPTO-ASSETS · EUROPEAN UNION

The EBA Sets Out What It Wants From the MiCA Review

On **24 September** the European Banking Authority published its response to the European Commission's targeted consultation on the review of MiCA — **recommendations to the Commission, not new rules**. For **third-country multi-issuer schemes** it recommends the Commission consider regulatory changes to mitigate “the significant to very significant risks” they pose. It also recommends clarifying MiCA's scope and definitions, considering regulating **crypto-asset lending, including where crypto-asset service providers facilitate access to decentralised lending protocols**, and reviewing the reporting framework. As at 1 September 2026, **39 EMTs** had been issued under MiCA and **0 ARTs** authorised.

SANCTIONS MAINTENANCE · UNITED STATES / DR CONGO

OFAC Consolidates Its Penalty Rules, and Delists a Congolese General

On **24 September** OFAC announced that it is consolidating information on **enforcement procedures and penalties** from individual parts of 31 CFR chapter V into a new part, the **Sanctions Penalties Regulations**, which will result in the **deletion of over 100 subparts**. The notice also removes and reserves a Syria-specific general license following the **rescission of Syria's designation as a State Sponsor of Terrorism**. On **23 September** OFAC removed **one individual and one entity** under its DR Congo programme — **François Olenga**, listed as Head of the Military House of the President, and **Safari Club**, linked to him — across eight SDN lines once aliases are counted. A delisting moves your screening results as surely as a designation does.

IDENTITY FRAUD · UNITED STATES / KOSOVO

The Rydax Marketplace Operator Pleads Guilty

On **24 September** the Justice Department announced that **Ardit Kutleshi**, 28, a Kosovar national, had pleaded guilty to **aggravated identity theft and money laundering conspiracy** for operating **Rydox**, a marketplace for cybercriminals to buy, sell and trade stolen personal information, access devices and cybercrime tools. Since at least 2016 Rydox conducted **over 7,600 transactions**, receiving **at least \$232,000** in revenue. Sentencing is set for 9 February 2027. What Rydox sold — stolen personal information and means of identification — is what onboarding identity checks exist to catch.

ASSET RECOVERY · UNITED KINGDOM

FCA Confiscation Orders After a £1.5m Crypto Investment Fraud

On **28 September**, at Southwark Crown Court, the FCA obtained confiscation orders against **Raymondip Bedi (£603,404.28)** and **Patrick Mavanga (£247,997.99)**, who between 2017 and 2019 cold-called consumers into fake cryptoasset investments; **at least 65 investors** lost **£1,541,799**. Orders under the **Proceeds of Crime Act 2002** require repayment of the benefit gained **or the value of available assets, whichever is lower**. The FCA says recovered funds will be returned to victims.

This Week's

3 Key Takeaways

01

A Supervisor Closed a Corridor, Not an Account

The CBUAE did not publish a fine this week. It prohibited every UAE branch of Bank Melli Iran from any financial transaction to and from Iran, trade finance and fund transfers included, citing examination findings and AML, CFT and proliferation-finance obligations. A measure like this does not appear in a sanctions feed; it appears in payment instructions and trade documents. Its own proliferation-finance guidance had already told institutions to watch Iran transactions associated with trade finance. If your institution touches those branches, the review starts with the flows, not the names.

02

Follow the Money Past the First Account

Four of this week's releases describe the same shape. The FCA found mule money usually cashes out between the second and fifth account, often by card. The Justice Department says over \$20 million passed through upwards of 57 accounts in the Cuban smuggling case, and that sextortion and romance-scam proceeds moved through peer-to-peer apps and crypto wallets before reaching Nigeria. Europol describes mobile phone shops allegedly set up to launder profits. Monitoring that stops at the first receiving account, or that treats card spend at a local business as ordinary, will miss the layer where these schemes cash out.

03

One of Our Six Spoke — and It Spoke Loudly

Across the six jurisdictions this digest follows, the only in-week financial-crime publication we could confirm from their own regulators was the CBUAE's action on Bank Melli Iran. The other UAE link this week came from Europe: Europol's account of fake IDs couriered from the United Arab Emirates. We checked the Saudi, Qatari, Mauritian and Moroccan regulators we can reach and found nothing on financial crime dated inside 22–28 September; several sites block automated access, so that is what we could see, not proof that nothing was published. We would rather say so than fill the space.

SonarPulse

AI-Powered Financial Crime Surveillance

Want this digest in your inbox every week?

Follow SonarPulse on LinkedIn · <https://www.linkedin.com/company/sonarpulse>

238,396

**SUSPECTED MULES'
ACCOUNTS CLOSED**

FCA survey · 23 Sept · figure for
2025, 35 firms

\$20M+

**THROUGH UPWARDS OF
57 ACCOUNTS**

DOJ · 25 Sept · Cuban smuggling
conviction

1,000+

**FAKE IDS, COURIERED
FROM THE UAE**

Europol · 23 Sept · allegedly, by a
Spain-based cell

10,000+

**ML AND PREDICATE
PROSECUTIONS**

FATF · 23 Sept · Türkiye mutual
evaluation

#FinancialCrime #AML #Sanctions #KYC #KYB #Compliance #RiskTech #SonarPulse

Sources: Central Bank of the UAE · US Department of Justice · Europol · UK Financial Conduct Authority · FATF · European Banking Authority · US Treasury / OFAC