SonarPulse

AI-POWERED FINANCIAL CRIME SURVEILLANCE

WEEK OF 10 – 16 NOVEMBER 2026

Financial Crime Weekly Digest

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

STORY OF THE WEEK

The DOJ moves against North Korea's crypto theft: FaceStealer infrastructure seized, and more than $1.2 billion of stolen Binance assets seized or restrained

ENFORCEMENT

NCA settlements worth around £55m in a Singapore laundering case · OFAC sanctions two Guatemalan trafficking groups · Operation TorNado: 354 dark web arrests

REGULATORY

OFSI's sanctions factsheet for overseas businesses · US bank agencies extend the third-party risk comment period · Operation Machinize goes year-round

STORY OF THE WEEK · UNITED STATES / NORTH KOREA

Freeze It Before It Moves.
The DOJ Hits Back at North Korea's Crypto Theft

$2.7B+

frozen so far by US government and private sector efforts, out of more than $6 billion in virtual assets the DOJ says North Korean actors stole from Binance

On **12 November** the Department of Justice announced coordinated actions against the North Korean government's schemes to fund its regime through the theft of cryptocurrency. The DOJ says that on or about 29 October members of the North Korean military, referred to by the FBI as **TraderTraitor**, stole more than $6 billion worth of virtual assets from the Binance exchange. Working with virtual asset service providers, US government and private sector efforts have so far frozen more than $2.7 billion, and the Department has court authorisation to **seize or restrain more than $1.2 billion** of that. Tracing continues as the actors launder through bridges, mixers and exchanges.

Separately, prosecutors in the Central District of California disrupted cloud-based infrastructure used in a social engineering scheme the FBI calls **FaceStealer**, which the DOJ says has resulted in the theft of more than $400 million in the last 18 months. Targets receive video-meeting invitations from accounts stolen from earlier victims; the hackers play prerecorded video of contacts the target knows, or deepfake videos of well-known figures in crypto and web3, then stage a fake technical error whose "fix" installs malware. Under a federal warrant the FBI seized over 900 webcam videos of victims.

- The DOJ says the FBI, with the Secret Service and IRS-CI, issued a Cyber Alert urging VASPs to block transactions with, or derived from, addresses TraderTraitor uses to launder the Binance assets
- FaceStealer now also targets people who develop and maintain open-source software, which the DOJ says appears calculated to enable software supply-chain attacks
- In several reported cases, the theft came several months to more than a year after the first compromise
- The FBI has published a report on how FaceStealer works, with protective steps and steps for victims

WHY IT MATTERS FOR COMPLIANCE TEAMS

This is a story about speed and screening. More than $2.7 billion was frozen because exchanges and other service providers acted on attributed addresses while the money was still moving. FaceStealer adds a second lesson: the account that invites you to a call may belong to a real contact and still be controlled by an attacker. Three questions for this week. **Can your team load a law enforcement list of wallet addresses the same day and block deposits derived from it? Do you trace exposure through bridges and mixers, not only direct transfers? And does your staff security training cover a video call from a trusted contact asking you to install a "fix"?**

ENFORCEMENT ACTIONS

Law Enforcement Strikes This Week

NATIONAL CRIME AGENCY · UNITED KINGDOM / SINGAPORE

£55m

Two More Settlements Worth Around £55m in a Singapore Laundering Case

On **12 November** the High Court approved settlements in which Haijin Su and Haika Xu, both linked to one of Singapore's largest ever money laundering cases, agreed to hand over around **£55m** of UK assets after NCA investigations. Under Unexplained Wealth Orders obtained in April and July 2025, the NCA froze approximately £45 million of Su's assets as the suspected proceeds of laundering from illegal gambling and overseas scam centres; he will surrender 75%, worth £35,187,285. In 2023 Xu bought 16 newbuild Soho flats for £24.7 million, without mortgages, through two UK companies set up expressly for the purchase. Faced with a UWO in June 2026, Xu chose to settle rather than answer; the settlement is worth £19,771,175 to the NCA. The NCA says it has now seized around £75 million from the same group in 12 months.

OFFICE OF FOREIGN ASSETS CONTROL · UNITED STATES / GUATEMALA / MEXICO

2 DTOs

OFAC Targets Two Guatemalan Trafficking Groups Working for Mexican Cartels

On **13 November** OFAC sanctioned the **Los Mendoza** drug trafficking organisation under E.O. 14059 and E.O. 13224, as amended, for providing material support to the Sinaloa Cartel, and **Los Huistas** under E.O. 13224, as amended, for supporting the Sinaloa Cartel and CJNG, both of which the US designated as Foreign Terrorist Organizations in 2025. Treasury says Los Mendoza is involved in contract killings and money laundering and has built economic interests through land dispossession, cattle ranching, agricultural businesses and real estate. Los Huistas was already designated under E.O. 14059 in March 2022; its updated SDN entry adds the SDGT tag and a secondary sanctions risk notice. In a concurrent action the State Department designated Los Lorenzanas as an FTO and SDGT.

US DEPARTMENT OF JUSTICE · EUROPOL · UNITED STATES / EUROPE / AUSTRALIA / NEW ZEALAND

354

Operation TorNado: 354 Dark Web Vendors and Buyers Arrested

Announced **12 November** by the DOJ's JCODE team and Europol: Operation TorNado, which ran from May 2025 to October 2026, led to **354 arrests**, including 132 in the United States and 59 in the United Kingdom. The DOJ reports the seizure of over **$234 million** in cash and virtual currencies and approximately 5.7 metric tons of drugs. Europol reports over EUR 60 million in cash and cryptocurrencies seized in European countries, and says its forensic and blockchain analysis teams traced illicit transactions. Europol lists the trends it saw: fragmentation of marketplaces, hybrid ecosystems where dark web forums and encrypted messaging services blur together, and rapid replacement of disrupted markets. FinCEN and OFAC were among the US partner agencies.

REGULATORY DEVELOPMENTS

Regulatory Moves
Reshaping the Compliance Landscape

UNITED KINGDOM

OFSI Publishes a Sanctions Factsheet for Overseas Businesses

On **12 November** OFSI added a two-page *Sanctions Factsheet for Overseas Business* to its UK financial sanctions guidance. It reminds firms that UK persons and companies are subject to UK financial sanctions **wherever they are in the world**, and that UK firms with overseas operations remain subject to them. Its checklist: screen relevant stakeholders and beneficial owners, not just the named entity, because evasion sometimes operates through layered ownership; understand what funds are for and where they are going; treat due diligence as ongoing; and check licence requirements. It notes that civil penalties apply on a strict liability basis, that criminal prosecution can lead to up to 7 years' imprisonment, and that being compliant with UK, EU or US sanctions does not mean being compliant with another regime.

UNITED STATES

US Bank Agencies Give Firms Until 16 December to Comment on Third-Party Risk Guidance

On **13 November** the FDIC, the Federal Reserve Board, the NCUA and the OCC extended to **16 December** the comment period for their proposed guidance on managing risks associated with third-party relationships; comments were originally due 16 November. The agencies describe the proposal as principles-based and, like all supervisory guidance, non-binding. When it is finalised, the federal bank regulatory agencies plan to rescind their existing third-party risk management guidance and replace it, and the NCUA plans to rescind its own. The Fed separately extended to 16 December the comment period on a proposed guide for Fed-supervised traditional community banks. This is still a proposal: nothing has been rescinded yet.

UNITED KINGDOM

Operation Machinize 3: 349 Arrests, and High Street Laundering Work Goes Year-Round

On **11 November** the NCA reported the results of the third Operation Machinize, a month of action through October 2026 with the National Police Chiefs' Council against money laundering and the criminal use of cash-intensive high street businesses: **3,029 premises** visited or raided, 349 arrests, £2.2m cash seized and £3.7m in account freezing orders. The NCA estimates that at least **£1 billion** of criminal cash is laundered each year through cash-intensive businesses such as vape shops and barber shops. Machinize now runs around the clock, 365 days a year, and its coordination cell, which used public and private data sharing including intelligence from financial institution partners, is now an enduring capability.

ON OUR RADAR

Watch This Space

MARKET ABUSE · FRAUD · UNITED KINGDOM

A £154m Fake Takeover Bid, Forged With Chat GPT, Ends in a Suspended Sentence

On **10 November** at Southwark Crown Court, Christopher Woolcott received a 2-year sentence suspended for 2 years, 200 hours of unpaid work and costs of £4,627.73, with 14 months for each of three forgery offences to run concurrently. The FCA says he built a stake in Touchstone Exploration, then launched a bogus bid to drive up its share price, inventing identities and forging takeover documents using Chat GPT; he stood to gain as much as £70,000. Investigators traced three phone numbers used by different supposed individuals to the same handset. Touchstone was not under investigation.

DRUG PROCEEDS · LUXURY ASSETS · UNITED STATES / MEXICO

36 Charged in a South Carolina Drug Trafficking and Money Laundering Case

Announced **10 November**: 36 individuals have been charged in a multi-state Homeland Security Task Force investigation into drug trafficking and money laundering. The DEA seized 346 kilograms of fentanyl, over $2.8 million, jewellery and 15 luxury vehicles, and secured notice of lawsuits on 17 properties in South Carolina and Georgia with an aggregate estimated value of nearly $4 million. The DOJ says a Mexico-based organisation has operated in South Carolina since at least 2011. Six defendants have pleaded guilty; for the rest, an indictment is merely an allegation.

FRAUD · SUPERVISION · UNITED STATES

OCC Risk Perspective: Super Intelligence in Attackers' Hands Amplifies Fraud Concerns

On **12 November** the OCC published its Semiannual Risk Perspective for Fall 2026, naming credit, market, compliance and operational risks as its key themes. Among the highlights, it says that advanced super intelligence, employed by threat actors, **amplifies cybersecurity and fraud concerns**, while banks of all sizes continue to explore ways to leverage it, with opportunities to enhance efficiency and internal controls. FaceStealer's deepfake video calls, in this week's lead story, are one example of what that looks like in practice.

This Week's 3 Key Takeaways

01 Be Ready to Act on Attributed Wallet Addresses Within Hours

The DOJ says US government and private sector efforts, working closely with virtual asset service providers, have frozen more than $2.7 billion of the stolen Binance assets, and the FBI has urged providers to block transactions with, or derived from, addresses the launderers use. Check how quickly a new law enforcement address list reaches your blockchain screening, whether it covers indirect exposure, and who can approve a freeze outside office hours.

02 Look Through the Named Entity

OFSI's new factsheet tells firms to screen stakeholders and beneficial owners, not just the named entity, because evasion sometimes operates through layered ownership. The NCA's Xu settlement shows the same pattern in a laundering case: 16 London flats bought without mortgages through two companies set up expressly for the purchase. A purchase made without finance through a newly created special-purpose company deserves a source-of-funds question.

03 Our Six: A Quiet Week, and a Factsheet Worth Forwarding

From the regulators of the UAE, Saudi Arabia, Qatar, Mauritius and Morocco we found no in-week financial crime item among the pages we could reach; ADGM's latest announcement was dated 9 November. Several of those sites block automated access, so that is what we could see, not proof that nothing was published. For firms in our region with UK links, OFSI's factsheet is worth forwarding: UK firms with overseas operations remain subject to UK financial sanctions, and local regimes may apply too.

SonarPulse

AI-Powered Financial Crime Surveillance

Want this digest in your inbox every week?

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

$2.7B+

STOLEN BINANCE ASSETS FROZEN SO FAR

DOJ · 12 Nov · "freeze of more than $2.7 billion"

354

ARRESTS IN OPERATION TORNADO

DOJ / Europol · 12 Nov · 132 in the US

£55m

UK ASSETS HANDED OVER IN TWO NCA SETTLEMENTS

NCA · 13 Nov · "around £55m"

£1bn+

CRIMINAL CASH LAUNDERED YEARLY THROUGH UK CASH-INTENSIVE BUSINESSES

NCA · 11 Nov · an estimate

#FinancialCrime #AML #Sanctions #KYC #Crypto #UWO #Compliance #SonarPulse

Sources: US Department of Justice · Europol · NCA · US Treasury / OFAC · OFSI · OCC · Federal Reserve · FCA · ADGM