Four African countries exit FATF grey list| FINTRAC levies largest ever fine on crypto exchange for AML deficiencies| Combating Romance Fraud and more

November, 2025

TOP STORY

Four African countries exit the FATF grey list

By Neha Treesa Joy

Four African nations, South Africa, Nigeria, Mozambique, and Burkina Faso, have been officially removed from the Financial Action Task Force (FATF) grey list, marking a major milestone in the continent's ongoing efforts to strengthen financial integrity and combat illicit finance. FATF, the global standard-setter for anti-money laundering (AML) and counter-terrorist financing (CTF) measures, made the announcement following its plenary meeting in Paris. These countries had been under increased monitoring, and they were working with the FATF to address identified strategic deficiencies in their AML/CFT frameworks.

South Africa and Nigeria were placed on the list in 2023, after Burkina Faso and Mozambique in 2021 and 2022, respectively. The FATF noted that all four countries had made significant progress in improving its AML/CTF systems. South Africa enhanced its ability to identify and investigate financial crimes, while Nigeria strengthened inter-agency coordination and regulatory enforcement. Mozambique improved financial intelligence sharing between authorities, and Burkina Faso bolstered its oversight of financial institutions and designated non-financial businesses and professions. These combined efforts were deemed sufficient for removal from increased monitoring.

Countries that remain on the FATF grey list need to take strong, coordinated action to strengthen their AML and CFT framework to meet FATF standards. Regulators need to prioritise high-risk sectors, such as casinos and real estate, which are often used to hide illicit funds. Ongoing enforcement, technological upgrades and public awareness are important measures to stay compliant and exit the grey list.

Source: Reuters

NEWS SNIPS FROM AROUND THE WORLD

[Collated from other publishers and sources from the Internet, as referenced after each snippet]

Myanmar Raid Exposes Cyber-Scam hub

The military in Myanmar captured a major cyber-scam compound known as KK park, which shares borders with Thailand. The park was linked to the Chinese mafia, uncovering a large-scale operation involved in online fraud, money laundering and human trafficking. Thousands of people were lured with the promise of well-paid jobs and reportedly forced to run scams targeting victims worldwide. Escaped victims described harsh conditions, where thousands of people, including many from African nations, were detained and forced to work long hours. KK Park is just one among at least 30 such compounds along the Thailand border.

Source: BBC

FIU-IND takes action against offshore Virtual Digital Asset Providers for non-compliance

The Financial Intelligence Unit (FIU-IND) has taken regulatory action against 25 offshore Virtual Digital Asset Service Providers (VDA SPs) for non-compliance under section 13 of the Prevention of Money Laundering Act (PMLA). FIU-IND has mandated the entities to take down their applications/URLs that have been found to be illegal. So far, 50 Virtual Digital Asset Service Providers (VDA SPs) have registered with FIU-IND. However, FIU-IND continues to identify entities serving Indian users that have not yet registered and therefore remain outside the AML/CFT regulatory framework. All VDA SPs, whether based in India or abroad, must register with FIU-IND as Reporting Entities if they engage in activities such as exchanging, transferring, or managing virtual digital assets.

Source: Press Information Bureau

FINTRAC levies largest ever fine on crypto exchange for AML deficiencies

Canada's anti-money laundering watchdog, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) has levied a record fine of C$176.9 million against money services business Xeltox Enterprises Limited. Xeltox failed to file suspicious transaction reports despite having reasonable grounds to suspect that certain transactions were linked to money laundering connected to child sexual abuse material. The company also neglected to report receiving over C$10,000 in virtual currency from a client. This move comes as the country prepares for an audit by the global financial crime watchdog, Financial Action Task Force (FATF).

Source: Reuters

Five sentenced for romance fraud and money laundering

Five men have been sentenced to prison in the UK after carrying out a large-scale romance fraud and money laundering operation that stole more than £2 million from unsuspecting victims. The gang targeted victims through online dating platforms, using fake identities and emotional manipulation to gain trust. Once relationships were established, they asked victims for money to cover invented expenses, including fines, travel emergencies, or urgent bills. Victims were persuaded to transfer funds into the men's bank accounts or, in some cases, to send cash through the post.

Source: BBC

83 arrested for terrorist financing in an INTERPOL and AFRIPOL coordinated operation

INTERPOL and AFRIPOL coordinated Operation Catalyst from July to September 2025 across six African countries to cut off terrorist financing sources. The operation exposed links between terrorism financing, fraud, cybercrime, and money laundering across multiple African countries. Investigators uncovered networks funnelling money through bank accounts, informal transfer systems, and virtual assets to support terrorist activities. More than 15,000 persons and entities were screened, revealing transactions worth an estimated USD 260 million linked to illicit activity, with about USD 600,000 already seized.

Source: INTERPOL

UK and US sanctions on a major fraud network

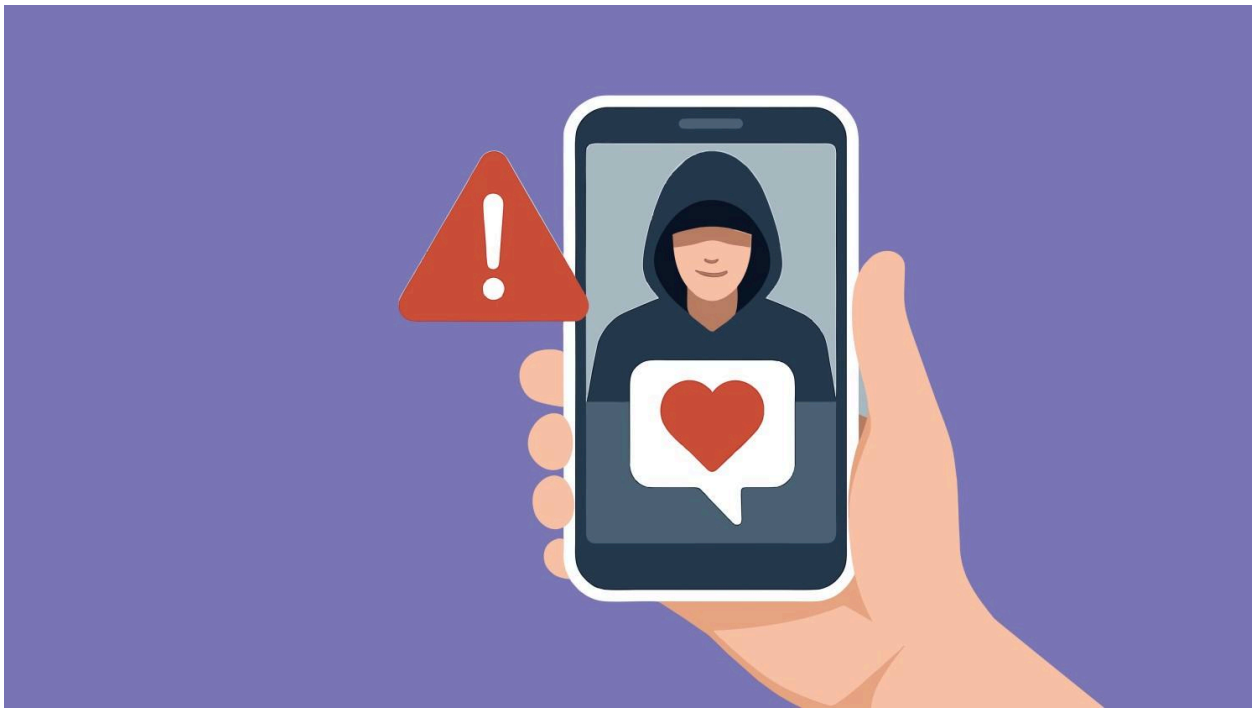
On 14 October 2025, the Office of Foreign Assets Control (OFAC) in the US and the Foreign, Commonwealth & Development Office (FCDO) in the UK jointly targeted a Southeast Asia-based online fraud network for sanctions. The network operated scam centres in Cambodia and Myanmar, using trafficked workers and conducting romance and crypto investment-based frauds globally. Proceeds were laundered through casinos, fake legitimate companies, and luxury UK real estate, including a £12 million London mansion and a £100 million city office. The sanctions will immediately block access to these businesses and properties.

Source: UK Government

DOMAIN MATTERS

Combating Romance Fraud: Findings from the FCA review

By Shivani S.



The Financial Conduct Authority (FCA), UK's financial regulator, recently published a report on combating romance fraud, outlining the key challenges, best practices, and areas for improvement in how financial firms detect, prevent, and respond to such cases.

Romance fraud typically involves scammers creating false online identities to build trust and emotional connections with victims under the pretence of a romantic relationship, ultimately aiming to deceive them for financial gain. The FCA's review covered six firms, including retail banks and payment providers, focusing on how they identify and prevent romance fraud while supporting affected customers.

Key challenges for institutions:

- Gradual trust-building: Scammers often develop relationships over weeks or months, slowly gaining victims' trust before requesting money. Since firms usually detect activity only once payments are made, early intervention is difficult.
- Low-value initial payments: Fraudsters usually begin by requesting small sums to appear credible and avoid suspicion. These transactions often blend in with normal spending patterns, making them difficult for firms to flag. Once a payee seems "trusted," later, larger payments are less likely to trigger warnings.
- Victims concealing the purpose of payments: In nearly half of the reviewed cases, victims did not reveal the true reason for their payments when questioned by their bank, limiting the firm's ability to identify and stop fraud effectively.

Best Practices for Detection and Monitoring:

- Manual intervention: Some firms effectively flagged and deferred suspicious payments for manual review, temporarily blocking transactions until customers confirmed them with a staff member. This approach introduced positive friction in the payment process, helping to prevent potential fraud.
- Detection of unusual payment patterns: Transaction monitoring systems that identified multiple payments to a new beneficiary within a short time frame proved effective.
- Multiple data points: The use of data points on the victim's profile, such as previously being a victim of fraud and attempted payments to a high-risk beneficiary with a history of fraud concerns can enhance monitoring.

Areas for Improvement:

- Fine-tune monitoring system: Firms should fine-tune their transaction monitoring systems to identify unusual or high-risk behaviour, ensuring that suspicious activity is promptly flagged for review.
- Financial distress indicators: Signs of financial strain or unusual borrowing should be considered as potential red flags, especially when combined with other risk factors.
- Due diligence: Some fraudsters instruct victims to open accounts in specific firms and move funds from their main bank to the new account, before transferring money to the fraudster. Firms receiving these funds should carry out proper due diligence on both incoming and outgoing transactions to prevent being used for fraud.
- Training: Continuous training and robust investigative processes can ensure alerts are being properly assessed and acted upon.

The FCA's review sheds light on the need for a multi-layered approach, including advanced detection systems, strong investigative procedures, and active staff engagement. While progress has been made, further improvements in using multiple data points, monitoring calibration, and cross-firm collaboration could help detect romance fraud at an earlier stage.

Source: Financial Conduct Authority

Navigate Consulting enables banks and financial institutions to better understand Financial Crime Management and make the most productive use of their AML and Fraud Management systems through training and knowledge sharing.

For more details write to: connect@navigate-change.com