OpenVoiceNews India

Transparent. Unbiased. Yours.

UK Sanctions Watchdog Warns on Crypto Risks

August 6, 2025
— Categories: Crypto

Download IPFS

The United Kingdom's Office of Financial Sanctions Implementation (OFSI) has issued a detailed 2025 Cryptoassets Threat Assessment, highlighting vulnerabilities in the sector that could be exploited to evade financial sanctions. The report, part of a series covering multiple industries, highlights the increasing regulatory scrutiny of digital assets amid heightened geopolitical tensions.

Under UK law, cryptoassets are subject to the same sanctions and anti-money laundering (AML) rules as other asset classes. Since January 2020, cryptoasset firms must register with the Financial Conduct Authority (FCA) for AML supervision under the Money Laundering Regulations and the Sanctions and Anti-Money Laundering Act 2018. The FCA has progressively expanded oversight, introducing the 'Travel Rule' in 2023, implementing a financial promotions regime, and publishing multiple discussion papers on stablecoins, market abuse, and broader crypto regulation. Draft legislation introduced in April 2025 seeks to bring trading platforms, lending, staking, and decentralised finance (DeFi) within the FCA's remit, with final rules expected in 2026.

OFSI's assessment identifies five core threats: underreporting of breaches, inadvertent non-compliance, Russian exposure, North Korean cyber threats, and Iranian connections. Over 90% of reported crypto-related suspected breaches since 2022 involve Russia, including potential links to the sanctioned exchange Garantex. Many breaches stem from indirect exposure to sanctioned individuals or entities, with delayed identification contributing to compliance failures. The report also warns of heightened risks from DPRK-linked hackers and potential transfers to Iranian cryptoasset firms with suspected sanctions links.

The report highlights high-risk practices enabling sanctions evasion, including the use of privacy tools, instant exchange services without Know Your Customer (KYC) checks, layering transactions across multiple blockchain networks, and darknet marketplaces. Over-the-counter (OTC) trades, decentralised exchanges (DEXs), and nested exchanges, which use another platform's infrastructure without permission, also present significant compliance challenges.

OFSI advises that two or more red flags should trigger enhanced due diligence. These include sudden changes in transaction patterns, exposure to known sanctioned entities, rapid asset movement across multiple wallets, repeated low-value payments from the same source, use of privacy coins or mixers, and transactions involving sanctioned jurisdictions.

To mitigate risks, OFSI urges firms to verify FCA registration of counterparties or check relevant overseas registers, use blockchain analytics to detect links to sanctioned parties, assess behavioural patterns and transaction histories, conduct retrospective reviews for unreported breaches, and report suspicious activity to OFSI, the FCA, and the National Crime Agency (NCA) without delay.

OFSI's report warns that cryptoasset firms face mounting compliance pressures as sanctions evasion techniques grow more sophisticated. The regulator calls for proactive risk management, enhanced monitoring systems, and close cooperation with authorities to prevent illicit financial activity. With the UK's regulatory regime set to expand, firms are urged to strengthen policies and training now to avoid enforcement action in the years ahead.