RAPID RESPONSE BRIEF

SANCTIONS COMPLIANCE AND CRYPTOASSETS IN THE UK

The last week has seen several updates from the UK Government, law enforcement, and the regulatory community relating to the ongoing Ukraine conflict and the efforts to impose financial sanctions on the Russian elite and their assets. These updates set out UK authorities' approach and expectations for the cryptoasset sector.

How does this relate to the Ukraine crisis?

- The United Kingdom, along with multiple jurisdictions and multilateral bodies, have imposed financial and trade sanctions on Russian individuals and entities as countermeasures to the Russian invasion of Ukraine.
- It is the responsibility of compliance officers and financial crime professionals to apply suitable measures to safeguard the implementation of government actions and maintain the integrity of the financial system.
- The cryptoasset sector in the UK and internationally has the same responsibilities as traditional financial institutions to apply money laundering and terrorist financing controls, and to ensure it is not breaching legislation relating to international sanctions lists.

UKFIU update for SARs containing sanctions related information

1. On March 10, 2022, the UK Financial Intelligence Unit (UKFIU) issued a notice to obliged entities under the UK Money Laundering Regulations setting out their expectations relating to Defence Against Money Laundering (DAML) and Defence Against Terrorist Financing (DATF) reporting. The note made clear that the DAML and DATF regime is distinct from the sanctions regime, but interacts with the sanctions

regime when sanctioned entities – and by extension persons not sanctioned but linked to sanction entities – are referred to by suspicious activity reports (SARs).
2. DAMLs and DATFs are not intended for reporting sanctions breaches (which should be reported to the Office of Foreign Sanctions Implementation (OFSI)). However, the identification of sanctioned entities, or linked non-sanctioned entities, may be made by the reporter and form part of the reasons for submission when submitting a SAR.
3. The note went on to remind reporters that, earlier in March, the UKFIU introduced a new SAR glossary code for entities associated with sanctioned individuals and companies on the sanctions list. Obliged entities should include the code **XXSNEXX** where they suspect the activity is consistent with money laundering and is linked to entities sanctioned by the UK, US, EU, and other overseas jurisdictions as a result of the Russian invasion of Ukraine.

Joint statement from the Financial Conduct Authority (FCA), HM Treasury's Office of Foreign Sanctions Implementation (OFSI), and the Bank of England (the Bank)

4. The statement (issued March 11) reiterates that all UK financial services firms, including the cryptoasset sector, are expected to play their part in ensuring that sanctions are complied with. Financial sanctions regulations do not differentiate between cryptoassets and other forms of assets. The use of cryptoassets to circumvent economic sanctions is a criminal offence under the Money Laundering Regulations 2017 and regulations made under the Sanctions and Anti-Money Laundering Act 2018.
5. The statement reminds cryptoasset service providers of their basic sanctions obligations (including when to freeze the funds of a designated person/entity) and urges them to enhance their sanctions controls (updating risk assessments, screening customer transactions, using blockchain analytics to identify high risk wallets, and gathering insights on typologies).
6. The statement also provides several specific sanctions evasion red flags, similar in nature to those issued by the Financial Crimes Enforcement Network (FinCEN) last week, including high risk jurisdictions, transactions with sanctioned wallet addresses, transactions with exchanges known to have poor financial crime controls, and the use of VPNs and/or mixers/tumblers.

Practical Steps for Compliance Professionals

- Firms should enhance their client risk rating tools to account for specific businesses or relationships. This could provide the opportunity to screen cryptoasset addresses related to sanctions.
- Updating your risk assessment to include a sanctions element and, where suitable, cryptoassets, allows an improved understanding of exposure to sanctions evasion and different forms of cryptoassets (including enhanced control assessment to check for specific features such as high-risk wallets).
- Knowledge and awareness are vital. Be aware of typologies, red flag indicators, thought leadership, and media articles outlining threats and vulnerabilities linked to sanctions evasion and cryptoassets.

Authors

Joby Carpenter, Global SME – Cryptoassets and Emerging Threats

March 15, 2022

About ACAMS

ACAMS is the largest international membership organization dedicated to providing opportunities for anti-financial crime (AFC) education, best practices, and peer-to-peer networking to AFC professionals globally. With over 90,000 members across 180 jurisdictions, ACAMS is committed to the mission of ending financial crime through the provision of anti-money laundering/counterterrorism-financing and sanctions knowledge-sharing, thought leadership, risk-mitigation services, ESG initiatives, and platforms for public-private dialogue. The association's CAMS certification is the gold-standard qualification for AFC professionals, while the CGSS certification is its premier specialist qualification for sanctions professionals. ACAMS' 60 Chapters globally further amplify the association's mission through training and networking initiatives. Visit acams.org/sanctions for more information.