Cooley

Trade Controls Update: UK Publishes Guidance on Cryptoasset Sector's Compliance With Financial Sanctions

August 12, 2025

On 21 July 2025, the UK Office of Financial Sanctions Implementation (OFSI) published guidance regarding sanctions compliance in the cryptoasset sector. The publication is an assessment of threats to UK financial sanctions in the sector and is intended to assist stakeholders with prioritization as part of a risk-based approach to compliance.

Who is considered a cryptoasset firm?

Cryptoassets are defined as 'any cryptographically secured digital representation of value or contractual rights that—(a) can be transferred, stored or traded electronically, and (b) that uses technology supporting the recording or storage of data (which may include distributed ledger technology)'. [1] Cryptoasset exchange providers and custodian wallet providers in the UK have needed to register with the Financial Conduct Authority (FCA) since January 2020. [2]

The report covers registered UK cryptoasset firms exchanging or arranging the exchange of cryptoassets for fiat (government-issued currencies) or vice versa, or of one cryptoasset for another (e.g., centralised exchanges, peer-to-peer providers and firms issuing new cryptoassets through, for example, initial coin offerings or initial exchange offerings), operators of crypto ATMs and custodian wallet providers.

How do financial sanctions apply to cryptoasset firms?

The prohibitions under each financial sanctions regime tend to include both asset freezes and prohibitions on making funds and economic resources available to individuals and entities listed in the sanctions regulation (so-called designated persons).

UK financial sanctions regulations do not differentiate between cryptoassets and other forms of assets, and using cryptoassets to circumvent financial sanctions is a criminal offence.

Cryptoasset firms have been added to the list of 'relevant firms' under the UK sanctions regime and as a result need to report to OFSI when they know or have reasonable cause to suspect they have encountered a designated person or a breach of financial sanctions regulations has occurred.

What is the current state of compliance?

According to the report, since January 2022, just more than 7% of all suspected breach reports submitted to OFSI involved cryptoasset firms. Yet, OFSI has identified inconsistent and delayed reporting as a key shortcoming in the current compliance efforts of cryptoasset firms. In particular, OFSI stated that the delayed attribution of recipients, including sometimes only retrospective identification, is leading to delayed reporting.

What are the most common compliance risks?

OFSI notes that designated persons have increasingly been exploiting cryptoassets to avoid restrictions imposed by sanctions. The report identifies the following common risks:

- **Geographies**: Among the cryptoasset-related suspected breach reports, more than 90% relate to the UK's Russia regime and the remaining 10% to the Iran regime. While Russia continues to be a priority, OFSI encourages cryptoasset firms to ensure robust compliance with **all** UK sanctions regimes.

- **Certain transaction arrangements and situations**: Transactions with the following characteristics were identified as being potentially suspicious: cross-border payments; centralised exchanges with links to designated persons; high-risk and non-KYC (know your customer) services; layering, mixing and anonymity-enhancing techniques; exchanges operating through darknet marketplaces; over the counter trades; use of decentralized exchanges (DEXs); and nested exchanges.

OFSI further warns of the threat of hackers linked to the Democratic People's Republic of Korea (DPRK) targeting UK-based cryptoasset firms, which 'present the most significant and persistent threat to the cryptoassets sector at present'. According to the report, DPRK-related actors have been responsible for multiple high-value cryptoasset thefts globally since 2022, including the theft of around US$1.5 billion in cryptoassets from an exchange in February 2025.

What should companies do to ensure compliance with financial sanctions?

To help companies identify situations when enhanced due diligence should be undertaken, the report sets out a number of red flags. These do not signify illicit activity in and of themselves, but can be indications of sanctions evasion or circumvention and therefore trigger enhanced due diligence. They include:

- Large or unusual transactions immediately following sanctions announcements.
- Repeated payments from individual addresses for very low amounts.
- Use of anonymity-enhanced cryptocurrencies (privacy coins) or technology, such as privacy wallets.
- Large cumulative volumes built from multiple small transfers (less than £10,000).
- Operating in jurisdictions that do not implement UK-aligned financial sanctions.
- Virtual private network (VPN) usage masking true geographic location of a counterparty.
- Counterparties refusing standard compliance checks or failing to provide transaction documentation.

The report also notes the risk that UK cryptoasset firms are currently likely facilitating transfers to Iranian cryptoasset firms with suspected links to designated persons. In relation to Russia, it notes that almost all transfers from attributed UK services or FCA-registered cryptoasset firms to designated persons since 2022 involved Garantex Europe OU (designated in 2022). While direct flows to Garantex have decreased significantly, indirect flows from UK entities to Garantex increased. Its domains and servers in Germany and Finland were seized, and around US$26 million in illicit cryptoassets were frozen following an international law enforcement operation in March 2025. OFSI warns that Garantex is now operating under the name of Kyrgyz-registered Grinex in an attempt to circumvent sanctions.

As far as practicalities for reporting are concerned, OFSI calls on cryptoasset companies making suspicious activity reports (SARs) to use the usual mechanism for reporting and:

- Include the inference 'OFSI – Cryptoassets Threat Assessment – 0725'.
- Bundle multiple small-value transactions involving the same actors or addresses into a single report, so long as this does not cause undue delay.
- Include certain details, including the identity of the designated person, addresses and crypto quantities. In the case of indirect transactions the route, for blocked transactions the measures put in place, and for transactions which already occurred the reason for the screening failure.

As a takeaway from this alert, companies that deal directly or indirectly with cryptoassets must verify and refine their processes to ensure full compliance with financial sanctions. If you would like any assistance or have any questions, contact any of the lawyers listed below.

[1] Financial Services and Markets Act 2000 (FSMA), as amended by the Financial Services and Markets Act 2023.

[2] See the full list.

Key Contacts

Juan Nascimbene London	jnascimbene@cooley.com +44 (0) 20 7556 4558
Caroline Hobson London	chobson@cooley.com +44 20 7556 4522
Rebecca Halbach Brussels	rhalbach@cooley.com +32 2 486 7503