Office of Financial
Sanctions Implementation
HM Treasury



Cryptoassets

Threat Assessment

July 2025

Office of Financial
Sanctions Implementation
HM Treasury

© Crown copyright 2025

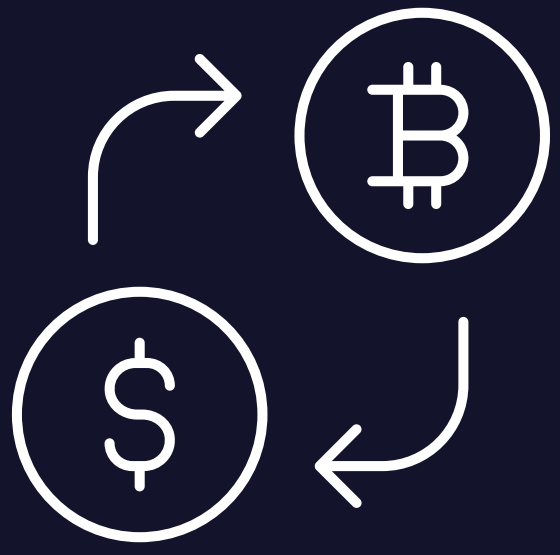
This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

Any enquiries regarding this publication should be sent to:
ofsi@hmtreasury.gov.uk

Contents

Introduction	4
Key Judgements	7
Threat Overview	8
Strengthening Compliance	11
Threats	20
Further Resources	32





Since January 2022, just over 7% of all suspected breach reports submitted to OFSI involved cryptoasset firms.

Introduction

This publication is one in a series of sector-specific assessments by OFSI addressing threats to UK financial sanctions compliance.[1] The UK sanctions landscape has changed significantly since the illegal Russian invasion of Ukraine in February 2022 and the subsequent implementation of unprecedented financial sanctions on Russia by the UK Government and international partners. Recognising the evolving nature of financial sanctions, OFSI is publishing this series of assessments to assist UK firms in better understanding and protecting against threats to compliance. These assessments also demonstrate OFSI's commitment to proactively investigate breaches of UK financial sanctions.[2]

This assessment provides information on suspected sanctions breaches only and is intended to assist stakeholders with prioritisation as part of a risk-based approach to compliance. In some cases, the activity described in this assessment would breach UK financial sanctions. This assessment is not necessarily a direct reflection of ongoing OFSI investigations or enforcement activity and is based on a wide range of information available to OFSI. The case studies provided on pages 27-31 of this assessment are fictional but draw on information available to OFSI.

OFSI assesses the seriousness of suspected breaches on their merits and determines what enforcement action is appropriate and proportionate on a case-by-case basis. Guidance on breaches of financial sanctions prohibitions and OFSI enforcement can be found here.

UK cryptoasset firms

This report outlines OFSI's assessment of threats to sanctions compliance involving UK cryptoasset firms since January 2022.[3]

The Financial Services and Markets Act 2000 (FSMA) (as amended by the Financial Services and Markets Act 2023) defines cryptoassets 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)." They are also sometimes referred to as digital assets or virtual assets.[4]

[1] This assessment covers UK financial sanctions only and does not cover UK trade sanctions, including the Russian Oil Price Cap, or those implemented by the Office of Trade Sanctions Implementation (OTSI). UK cryptoasset firms should also consider their obligations relating to compliance with trade sanctions. Further information is available here.

[2] OFSI works closely with the National Crime Agency (NCA), which is responsible for investigating suspected criminal breaches of UK financial sanctions.

[3] The content of this assessment is based on information reviewed by OFSI from between January 2022 and May 2025.

[4] See Section 417 of the Financial Services and Markets Act 2023. https://www.legislation.gov.uk/ukpga/2023/29/section/69.

Financial sanctions regulations do not differentiate between cryptoassets and other forms of assets. Financial sanctions regulations therefore apply to cryptoassets in the same way they do to other forms of assets. The use of cryptoassets to circumvent financial sanctions is a criminal offence under the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs) and regulations made under the Sanctions and Anti-Money Laundering Act 2018 (SAMLA).

The Financial Conduct Authority (FCA) is the anti-money laundering and counter-terrorist financing supervisor for cryptoasset firms and other financial institutions in the UK. From January 2020, cryptoasset exchange providers and custodian wallet providers, as defined in the MLRs, have needed to register with the FCA for MLRs supervision.

For the purposes of this assessment, UK cryptoasset firms are all UK businesses registered with the FCA that conduct the following types of cryptoasset business activity:[5]

- Exchanging, or arranging or making arrangements with a view to the exchange of, cryptoassets for fiat or fiat for cryptoassets, or of one cryptoasset for another; (e.g. centralised exchanges; Peer-to-Peer Providers; and firms issuing new cryptoassets, e.g. through Initial Coin Offerings or Initial Exchange Offerings);
- Operating a machine which utilises automated processes to exchange cryptoassets for money or money for cryptoassets (crypto ATMs) and;
- Providing services to safeguard and/or administer cryptoassets or private cryptographic keys to hold on behalf of customers in order to hold, store and transfer cryptoassets (custodian wallet providers).

A full list of registered and formerly registered UK cryptoasset firms is provided by the FCA.[6] OFSI encourages all firms operating in the UK or firms engaging with UK customers to check the FCA register to identify whether any cryptoasset firms they do business with are registered, or to check the equivalent register of the jurisdiction in which the cryptoasset firm is based. Since September 2023, the UK also applies the 'Travel Rule', which requires UK cryptoasset firms to collect, verify and share information about the sender and receiver of cryptoasset transfers.[7] The FCA's Crypto Roadmap outlines planned policy publications for cryptoassets for the ongoing regulation of the UK's growing cryptoassets sector.[8]

[5] For more information, see Cryptoassets: AML / CTF regime | FCA.
[6] For more information, see Registered Cryptoasset Firms.
[7] For more information, see FCA sets out expectations for UK cryptoasset businesses complying with the Travel Rule | FCA.
[8] For more information, see FCA Crypto Roadmap.

The Bank of England prudentially regulates and supervises UK financial services firms, including cryptoasset firms, through the Prudential Regulation Authority (PRA).

Reporting to OFSI

In August 2022, cryptoasset firms were added to the list of 'relevant firms' in sanctions regulations. This means cryptoasset firms are now obliged to report certain information to OFSI when (within the course of their business) they:

- Know or have reasonable cause to suspect they have encountered a designated person (DP);[9]
- Know or have reasonable cause to suspect a breach of financial sanctions regulations has occurred.

Reporting any suspected sanctions breaches to OFSI is essential as it provides the government with vital information about the activities of DPs and the presence of frozen assets – including cryptoassets – in the UK.

Further information about reporting to OFSI can be found here. OFSI encourages firms to report if they suspect a breach linked to the content of this assessment has occurred. Where appropriate and proportionate, OFSI encourages firms operating in the cryptoasset sector, and firms in all sectors, including financial services, to conduct lookback exercises to identify any past suspected breaches involving cryptoassets which might not have been reported to OFSI. It will assist OFSI if firms reference "OFSI – Cryptoassets Threat Assessment – 0725" in any report.[10]

Suspicious Activity Reports (SARs)

If you know or suspect that there has been money laundering or terrorist financing activity and your business falls within the regulated sector, then you are reminded of the obligations to make reports to the National Crime Agency (NCA) under Part 7 of the Proceeds of Crime Act 2002 and the Terrorism Act 2000. If you decide to make a report in this way, you should adopt the usual mechanism for doing so. It will help analysis if the reference "OFSI – Cryptoassets Threat Assessment – 0725" is included. Guidance on SARs is available here.

[9] The requirement to report knowledge or reasonable cause to suspect that a person is a DP applies in relation to persons designated under the asset freeze etc. (and so on the OFSI Consolidated List). Otherwise, in this Threat Assessment, unless indicated to the contrary, Designated Persons (DPs) includes both individuals and entities listed on the OFSI Consolidated List and persons owned and controlled by entities and individuals on the OFSI Consolidated List.
[10] Further information on what could prompt this can be found in the Red Flags section of this report (pp. 16-19).

Key Judgements

This assessment concerns sanctions threats relevant to UK cryptoasset related services firms from January 2022 to May 2025.

1. It is **almost certain** that UK cryptoasset firms have under-reported suspected breaches of financial sanctions to OFSI since August 2022.

2. It is **likely** that most non-compliance by UK cryptoasset firms has occurred inadvertently due to common issues such as direct and indirect exposures to DPs and suspected breaches being identified after a delay in attribution, with attribution delays also contributing to failures to implement the asset freeze.

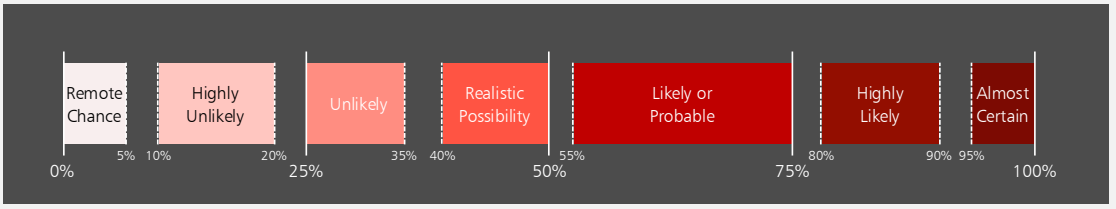
3. It is **highly likely** that UK cryptoasset firms have been directly or indirectly exposed to the designated Russian exchange Garantex since its designation in 2023, resulting in breaches of UK financial sanctions.

4. It is **highly likely** that UK-based cryptoasset firms are currently at risk of being targeted by DPRK-linked hackers and IT workers seeking to steal or obtain funds through illicit means.

5. It is **likely** that UK cryptoasset firms are currently facilitating transfers to Iranian cryptoasset firms with suspected links to DPs.

Probability Yardstick

This assessment uses probabilistic language as detailed in the Probability Yardstick developed by HMG's Professional Head of Intelligence Assessment.

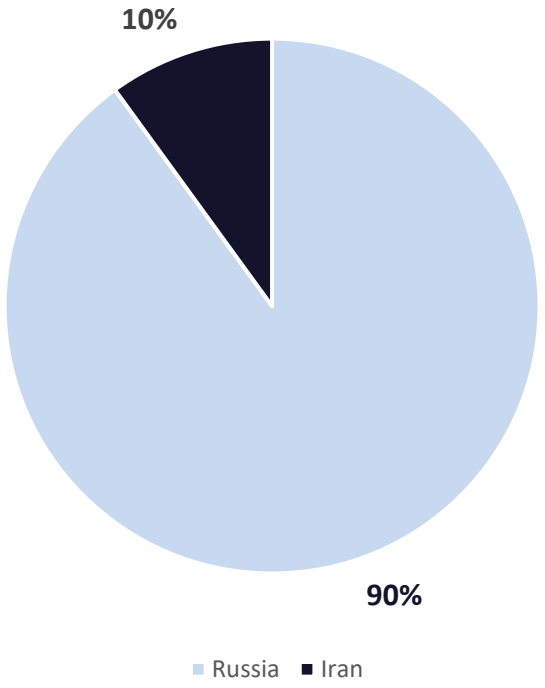


Threat Overview

A breakdown of suspected breach reports involving UK cryptoasset firms submitted to OFSI since January 2022 is provided below.[11]

Suspected breach reporting by regime

Russia accounts for over 90% of cryptoasset-related suspected breach reports made to OFSI since January 2022, with Iran making up the remaining 10%. While Russia sanctions remain a priority, OFSI encourages cryptoasset firms and all firms that transact with firms in the cryptoassets sector to ensure robust compliance with all UK sanctions regimes. This is particularly relevant for cryptoassets firms and service providers, given the transnational nature of the sector.



[11] This data is based on suspected breaches reported to OFSI between January 2022 and April 2025 inclusive.

Suspected breach reporting by UK cryptoasset firms

1. It is **almost certain** that UK cryptoasset firms have underreported suspected breaches of financial sanctions to OFSI since August 2022.

OFSI closely monitors suspected breach reports on a sectoral basis to identify patterns of non-compliance. Since January 2022, just over 7% of all suspected breaches reported to OFSI involved cryptoasset firms in some capacity. The vast majority of these reports (over 90%) were made since April 2024. Despite this significant increase in suspected breach reports, OFSI notes that reporting has been inconsistent and has observed in some cases significant delays in both identifying suspected breaches and subsequently making reports to OFSI. In particular, OFSI has observed that delayed attribution of recipients is leading to delayed reporting.

OFSI values self-disclosure and timely reporting of suspected breaches (further information on this can be found here). OFSIproactively investigates suspected breaches which are not directly reported to OFSI using a wide range of available information. When self-disclosing a suspect breach, cryptoasset firms should, in addition to reporting to OFSI, also report to other authorities where relevant (including through SARs and to the FCA).

Most reporting by UK cryptoasset firms to date has related to transactions involving designated exchanges. OFSI notes that exposure to sanctioned entities is often complex in nature and that UK cryptoasset firms can incur wider sanctions risks, including through exposure to cryptoasset addresses known to be owned or controlled by DPs, such as those cryptoasset addresses published on the OFSI Consolidated List; through exposure to cryptoasset addresses suspected to be owned or controlled by DPs, but where the cryptoasset addresses are not listed on the OFSI Consolidated List; or through breaches that arise in situations where DP clients of UK cryptoasset firms are involved in transactions that would otherwise be prohibited by sanctions.

OFSI has seen that UK cryptoasset firms sometimes identify transactions made to sanctioned entities significantly after they have occurred (i.e. the addresses are attributed significantly after they were executed) or retrospectively once a firm gains access to blockchain analytics software. This has resulted in delays in making reports to OFSI. While OFSI has noted an improvement in the timeliness of reporting suspected breaches by UK cryptoasset firms, with the difference between the time of discovery and the time of reporting by UK cryptoasset firms gradually reducing over the past 12 months, reporting inconsistencies remain across the sector. To mitigate against this, and to address industry

questions about reporting obligations, OFSI is issuing the below set of recommendations with the aim of clarifying what constitutes best-practice reporting in this sector.

When reporting suspected breaches to OFSI (including when self-disclosing), UK cryptoasset firms and firms in any sector interacting with them should consider the following:

- Where multiple small-value transactions involving the same actors or addresses are referenced, these should be bundled together and a single report should be made, with an accompanying explanation of why they were so grouped. Grouping should however only be done where doing so would not cause undue delay.
- Where transactions are referenced, the involved addresses, including intermediary addresses, transaction hashes and crypto quantities (with USD/GBP value) should be listed. If the value of transactions exceeds 1000 GBP, the involved addresses should be included at a minimum.
- If a transfer is suspected to have originated from or been made to a DP, the DP should be specifically identified, as well as the rationale for linking the specified addresses to that DP (e.g. through blockchain analytics attribution).
- If the transaction is historical (i.e. took place considerably before the reporting), the delay in identification and reporting should be explained.
- If the transaction was indirect (i.e. not one hop to a DP), a description of the route, including statement of these intermediary addresses, should be included.
- If a transaction to a DP was allowed, this failure in screening should be explained (e.g. third-party blockchain analytics tool did not cluster the address at the time). If it was blocked, include what steps have been taken to prevent onward transmission or access.
- If the assets involved in a suspicious transaction have been frozen or moved elsewhere (if the reporter was the receiver), such as if the crypto was cashed out to a bank account after the transaction occurred.
- Know Your Customer (KYC) details of the individuals involved in the suspected offending transaction, with name, date of birth, and account number as a priority.
- A brief summary of the crypto screening process used and of the detection and escalation process, including how these decisions were made.
- Any action already taken by the reporter (e.g. account closure or restrictions put in place as part of a risk-based approach to compliance).

OFSI urges UK firms to also report any suspected illicit activity involving cryptoassets to the NCA and the FCA where relevant, as per their legal obligations, using the usual reporting mechanisms.[12]

Strengthening compliance

2. It is **likely** that most non-compliance by UK cryptoasset firms has occurred inadvertently due to common issues such as direct and indirect exposures to DPs and suspected breaches being identified after a delay in attribution, with attribution delays also contributing to failures to implement the asset freeze.

OFSI has reviewed a wide range of information, including suspected breaches, to identify threats to financial sanctions and understand how compliance by UK cryptoasset firms could be strengthened. In addition to the specific threats outlined in this assessment, this assessment highlights common compliance vulnerabilities, including:

Direct or indirect exposure to a DP. Exposure to DPs or associated clusters, either direct or indirect, constitutes the main threat to sanctions compliance currently impacting the UK cryptoassets sector. For the purposes of this assessment, direct exposure to a DP through cryptoassets occurs when a person or entity has a clear, identifiable relationship with a DP. This includes transacting directly with a wallet address that is owned or controlled by a DP, providing services (e.g., exchange, custody, payment processing) to a DP, or receiving cryptoassets from, or sending cryptoassets to, a wallet that is owned, held or controlled by a person on the OFSI Consolidated List.[13] Non-compliance through direct exposure occurs when firms do not identify that an end-user address is associated with a DP. However, UK cryptoasset firms face sanctions compliance risks even when they do not directly transact with DPs. Indirect exposure situations can occur when cryptoassets pass through one or more intermediaries after originating from a DP's wallet (sometimes called "layering"), or by receiving cryptoassets that have been mixed or tumbled, making it difficult to trace their origin back to a DP.[14] It can also occur when a firm provides services to customers who have direct dealings with a DP, even if the service provider does not interact with the DP directly. Specifically, indirect exposure to DPs can occur when:[15]

- A cryptoasset firm receives assets that previously passed through a DP's wallets
- A cryptoasset firm uses cloud services, software, or hardware from sanctioned jurisdictions

[12] For more information, see Suspicious Activity Reports - National Crime Agency and Report wrongdoing or misconduct in financial services | FCA.
[13] OFSI Consolidated List Search
[14] Mixing or tumbling is a process that obscures the transaction history of cryptoassets by pooling funds from multiple users and redistributing them, making it difficult to trace the original source of the assets.
[15] This list is not exhaustive.

- Smart contracts interact with exchanges or services in sanctioned jurisdictions
- Customers of cryptoasset firms use Virtual Private Networks (VPNs) to mask their true location and hide links to DPs
- Beneficial ownership structures obscure links to DPs
- Trading systems inadvertently provide liquidity to DPs
- DPs participate anonymously in Decentralised Finance (DeFi) protocols[16]
- A nested exchange cluster of deposit / withdrawal wallets sits under one fully verified customer account at a large, regulated cryptoasset exchange. The nested exchange markets itself as an independent service offering quick swaps and minimal KYC checks.

	Description	Example
Direct exposure	Direct interaction with a DP's wallet/ DP.	Sending/receiving crypto from a DP's wallet address.
Indirect exposure	Involvement via intermediaries or obfuscated transactions (e.g. via bridge).	Cryptoassets received after mixing, originally from a DP.

Both direct and indirect exposures to DPs are likely to result in breaches of UK financial sanctions. A "hop" is a single transaction between two addresses on a blockchain. Multiple hops create a chain of transactions.

1 hop: Designated Address A → End-user Address B
2 hops: Designated Address A → Intermediate Address C → End-user Address B
3 hops: Designated Address A → Address C → Address D → End-user Address B

Chain-hopping can occur in several ways:

- Through a simple chain
- Through cryptoasset exchanges, where each platform transfer counts as a hop
- Through DeFi interactions, where each smart contract interaction counts as a hop
- Through mixing or tumbling services specifically designed to increase hop distance

OFSI recommends that UK cryptoasset firms scan 3-5 hops minimum in transaction history or until the cryptoassets reach an attributed service provider and report any suspicious

[16] Decentralised Finance (DeFi) protocols are blockchain-based financial applications that allow users to lend, borrow, trade, and earn interest on cryptoassets without traditional banks or intermediaries.

activity to OFSI as soon as it is discovered. For example, if a firm discovers that cryptoassets have entered a mixer under circumstances suspected to be linked to sanctions evasion activities, they should immediately report this to OFSI, along with the address they entered through. OFSI also notes that blockchain immutability means exposure to a DP never truly disappears, as more hops do not eliminate exposure fully - they just make it more challenging to detect. Blockchain analysis tools can trace connections across hops through the entire blockchain when investigating suspected sanctions breaches. OFSI urges cryptoasset firms to take a risk-based approach to compliance, considering relevant factors including counterparty risk, behavioural patterns and transaction history depth based on the number of hops. When assessing the risk of a service, it is important to consider the category that service belongs to and, where possible, make comparisons to similar entities.

Retrospective discovery of suspected breaches. Post-designation, a DP may attempt to move their cryptoassets to distance themselves from links to known cryptoasset addresses. These transactions are visible on the blockchain (e.g. through blockchain analytics tools, which can help identify new addresses used by the DP). However, where a cryptoasset firm only monitors for incoming cryptoassets linked to the initial sanctions designation, it may not detect new addresses used by a DP and will therefore remain unaware of the risk level of incoming cryptoassets. In these cases, there is a realistic possibility that potential sanctions breaches related to the DP will remain unidentified and therefore lead to non-compliance. This represents a systemic vulnerability. OFSI urges cryptoasset firms to monitor for any new addresses linked to DPs through blockchain analytics.

OFSI notes that cryptoasset firms that identify transactions involving DPs after they occurred (i.e. in cases where the addresses are attributed at a later point, or where historical breaches are discovered after the acquisition of clustering blockchain analytics tools) should still report suspected breaches to OFSI, and as appropriate to the FCA and the NCA via the usual reporting channels as soon as the suspected breach is discovered. Blockchain analytics tools may also flag historical transactions that occurred before an entity or individual was designated. When these tools are updated to reflect new sanctions designations, they can retrospectively identify and flag previous direct or indirect exposure to virtual addresses of persons who were subsequently sanctioned, even though this activity was legitimate at the time it occurred. These transactions do not need to be reported to OFSI unless they are connected to suspected breach activity post-designation. If in doubt about whether an activity occurred before or after designation, a report should be made.

Management of frozen funds or economic resources. Cryptoasset firms cannot reject incoming transactions. When incoming cryptoassets are linked to suspected sanctions evasion or contravention activities, including (but not limited to) where firms suspect that transfers have been made so as to ultimately provide funds or economic resources to a

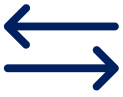
DP, UK cryptoasset firms should restrict users from accessing an account and transferring those assets. While holding custody of virtual assets tied to suspected sanctions evasion or circumvention activity, UK cryptoasset firms should report the suspected activity to OFSI. Where there is no applicable exception or licence then DP assets, including those tied to suspected breach activity, should be frozen and reported to OFSI as part of frozen asset reporting. If such activity is noticed and the firm operates within the regulated sector, a SAR report should also be filed with the NCA through the usual reporting channels.

Transactions involving cryptoassets occur at a faster pace than traditional financial transactions. Firms should take a risk-based approach to compliance and consider the use of specialised software to conduct blockchain analysis as part of their due diligence processes to capture transaction screening across multiple stages. Assessing counterparty exposure, including by using geolocation tools, can help identify an entity's exposure to illicit activity alongside other complementary screening processes. OFSI urges UK cryptoasset firms to report suspicious transaction chains to OFSI as soon as they are discovered.

Typologies



Cross-border Payments: Cryptocurrencies enable international trade and payments, circumventing traditional financial channels and sanctions compliance mechanisms, allowing direct payments to and from users in sanctioned jurisdictions. This can include the use of less regulated exchanges and services based in jurisdictions that do not implement financial sanctions aligned with the UK's or do not cooperate with UK law enforcement. OFSI notes the increased use of VPN services by sanctions evaders to obfuscate their true location.



Centralised Exchanges with Links to DPs: Certain centralised exchanges continue to operate cooperatively with designated exchanges, despite sanctions levelled against them. Supposedly separate entities may operate using shared infrastructure, employing obfuscation techniques, like disguising withdrawals and using intermediary wallets, to separate incoming deposits from withdrawals and circumvent compliance software that flags links to a DP.



High-Risk and Non-KYC Services: Some Russian-language, non-KYC instant-exchange services are used for quick fiat-to-crypto transactions, which facilitate sanctions evasion by moving funds from sanctioned individuals and entities (including sanctioned banks) to specified crypto wallets, without collecting customer information.



Layering, Mixing and Anonymity Enhancing Techniques: Sanctions evaders often use so-called mixing services (sometimes also referred to as tumbling services) to obscure transaction pathways and payment structures. This may involve laundering stolen crypto through multiple steps. Anonymity-enhancing technology such as privacy wallets are increasingly being used for money laundering purposes. Mixers enabled by smart contracts on DeFi protocols add a further layer of obfuscation by removing any human interaction with cryptoassets. Layering assets through cross-chain movement - also known as chain hopping – enables users to move cryptoassets between different blockchain networks using "bridges," making transactions harder to follow. This technique is commonly used to increase the complexity of tracing illicit cryptoassets across public blockchains.



Exchanges Operating through Darknet Marketplaces: Known as dark web or darknet forums, these are platforms where individuals can discuss, sell, and promote illicit activity, including sanctions evasion, anonymously. They derive their income from registration fees, advertisements, escrow services and account status upgrades.



Over the Counter (OTC) Trades: Used to convert cash into cryptoassets and vice versa, OTC trades can occur through Peer-to-Peer (P2P) transactions, via an OTC trading desk or through direct broker-facilitated arrangements.[17] As OTC trading activity often takes place outside of the supervision of an exchange, it is less regulated than usual exchange-based trades, and can be used to facilitate illicit activity, including money laundering and sanctions evasion. OTC broker-facilitated trades operate internationally and can be used by sanctions evaders to exchange cash in one jurisdiction and access it in another, enabling cross-jurisdictional movement of assets that may be otherwise prohibited.

[17] No P2P trading platforms are currently registered with, or permitted by, the FCA.



Use of Decentralised Exchanges (DEXs): DEXs are trading platforms that provide cryptoasset transactions between two parties. They are run on smart contracts that handle trades automatically using an underlying liquidity pool. DEXs require no identity checks and can facilitate pseudonymous trading, making them attractive to sanctions evaders.[18] Most DEXs operate as decentralised protocols without a single controlling entity for compliance or law enforcement purposes.



Nested Exchanges:[19] They operate by using larger exchanges' infrastructure to offer trading services, sometimes without the host platform's awareness or approval. Research indicates these exchanges handle illicit cryptoassets at much higher rates than legitimate platforms.

Other sector-wide threats include:

- The use of non-standard tokens, such as vouchers, can represent a form of sanctions evasion, as these are not as easily traced as conventional cryptocurrencies.
- The use of meme coins can potentially increase in value over time. They can also be artificially inflated or used as proxies for value.
- The use of Non-Fungible Tokens (NFTs) can contribute to sanctions evasion if DPs' cryptoassets are converted into digital collectibles that can be transferred across borders without traditional oversight, exploiting subjective valuations and regulatory gaps.

Red Flags

Cryptoasset firms and UK firms operating in other sectors that deal with the cryptoassets sector can strengthen compliance with UK financial sanctions by ensuring robust due diligence is conducted. In suspected breaches reported to OFSI since January 2022, OFSI has observed some instances of insufficiently detailed due diligence checks. Based on this and other available information, OFSI has observed several common red flags in this sector. While these red flags do not signify illicit activity in and of themselves, they could be indicative of sanctions evasion or circumvention, especially when two or more are present, and should trigger increased due diligence.[20]

---

[18] For the purposes of this assessment, pseudonymity means that while public wallet addresses are visible on the blockchain, the identities of their holders are not linked to those addresses.
[19] Nested exchanges are sometimes also referred to as "parasite" exchanges.
[20] Further information about the types of situations where these red flags could arise is provided in the case studies provided on pp. 27-31.

- Large or unusual transactions immediately following sanctions announcements
- Exposure to counterparties with known associations to DPs
- Sudden changes in transaction patterns, which may indicate attempts to circumvent compliance measures or otherwise obfuscate on-chain activity
- Repeated payments from individual addresses for very low amounts
- Rapid movement of assets through multiple addresses
- Newly created wallets receiving large transfers, or dormant wallets with no prior transaction history suddenly becoming active
- Multiple wallets controlled by the same entity (address clustering)
- Increasing reliance on DEXs over regulated exchanges
- Exposure to services lacking a KYC requirement or transactions involving services that do not require user identification
- Exposure to services lacking Anti-Money Laundering procedures
- Frequent address changes
- Use of anonymity enhanced cryptocurrencies (privacy coins)
- Use of anonymity-enhancing technology such as privacy wallets

	Use of mixing/tumbling services
	Use of OTC brokers or trading platforms
	Use of P2P exchange services
	Cross-chain bridge usage to obscure transaction trails
	Cross-chain transfers (chain hopping), particularly to privacy-focused blockchains
	One customer account generating hundreds / thousands of new deposit addresses via Application Programming Interface (API)[21]
	Concentrated inflows from mixers, darknet or ransomware wallets, followed by immediate withdrawals
	Large cumulative volumes built from multiple small (<£10 k) transfers
	Public marketing of "no-passport cash-out" or "sanctions-proof" services on social media
	Operating in jurisdictions that do not implement UK-aligned financial sanctions
	Transactions originating from or directed to sanctioned jurisdictions

[21] An API is a protocol that enables applications to interact with cryptoasset platforms and blockchain networks to access data and execute transactions.

	VPN usage masking true geographic location of a counterparty
	Counterparties refusing standard compliance checks or failing to provide transaction documentation
	Inconsistent or unexplained source of assets explanations
	Frequent migration of technical infrastructure (e.g. on a daily/weekly basis)

OFSI works alongside other Government agencies to coordinate a joint approach to tackling the threat to sanctions posed by illicit activity involving cryptoassets, including through shared resources and coordinated action.

Threats

OFSI assesses that since 2022, DPs have increasingly used cryptoassets to bypass sanctions, exploiting the pseudonymous and borderless nature of blockchain transactions. OFSI identifies the below trends as posing a threat to the integrity of UK financial sanctions.

Exposure to Russian DPs

3. It is **highly likely** that UK cryptoasset firms have been directly or indirectly exposed to the designated Russian exchange Garantex since its designation in 2023, resulting in breaches of UK financial sanctions.

Direct or indirect exposure to Garantex

Since 2022, OFSI has noted a significant proportion of transactions facilitated by UK cryptoasset firms to the Russian cryptoasset exchange GARANTEX Europe OU (Garantex). Garantex was designated by the UK in May 2022 under the Russia (Sanctions) (EU Exit) Regulations 2019 for its involvement in obtaining a benefit from or supporting the Government of Russia by carrying on business in the financial services sector, a sector of strategic significance to the Government of Russia.

According to information available to OFSI, almost all transfers from attributed UK services or FCA-registered cryptoasset firms to DPs since 2022 involved Garantex. On-chain analysis of Garantex found that the exchange received significant amounts from a variety of illicit activity during this time, including but not limited to ransomware groups. Garantex was also a key financial conduit for Hydra Market, the largest darknet marketplace in history, before its takedown.

While prior to 2022, the main services interacting with Garantex were centralised cryptoasset exchanges, OFSI has observed a diversification in the type of services exposed to Garantex post-designation, with a rise in interactions with merchant services. OFSI notes that since its designation in 2023, direct flows from UK cryptoasset firms to Garantex have decreased significantly. This has likely occurred as a result of Garantex shifting its internal infrastructure since being designated, making it harder to identify deposit addresses and hot wallets. During the same timeframe, indirect flows from UK entities to Garantex increased.

Recent reporting by the NCA demonstrates how Russian money laundering networks with

links to Serious Organised Crime groups used cryptoassets to breach financial sanctions implemented by the UK Government and international partners. Operating internationally, one such group was found to have provided a variety of services, including a system for the exchange of cash to crypto (and vice versa). The NCA noted that cryptoassets and cash couriers played a central role in these activities, and that Russian money laundering groups had significant exposure to Garantex. The groups also extensively exploited dollar-backed stablecoins such as Tether (USDT).[22]

Stablecoins are virtual assets that are backed by specified assets – generally fiat currencies – and therefore have less price volatility than other virtual assets. They can be used for buying or selling cryptoassets and making near-instantaneous cross-border payments. Most commonly used stablecoins, like USDT or DAI, are pegged to USD.

OFSI assesses that Russian P2P trading platforms are likely facilitating sanctions circumvention by avoiding direct transactions with designated Russian exchanges, thus bypassing due diligence and KYC checks.

In March 2025, Garantex was disrupted as part of an international law enforcement operation, resulting in the seizure of its domains and servers in Germany and Finland and the freezing of ~26 million USD in illicit cryptoassets. Criminal charges were filed against two Garantex administrators for laundering several hundred million dollars in cryptoassets.[23] Since its disbandment, OFSI assesses that it is highly likely that at least one successor organisation has been set up and is currently operating as a direct continuation of Garantex.

[22] NCA Operation Destabilise press release, published 4th December 2024.
[23] For more information, see Office of Public Affairs | Garantex Cryptocurrency Exchange Disrupted in International Operation | United States Department of Justice.

Emergence of Grinex

According to information available to OFSI, since its takedown in March 2025, Garantex has continued its operations using a new name. Grinex is a Kyrgyz-registered crytoasset service provider offering conversion between USD, Ruble, USDT and A7A5, a Ruble-backed stablecoin. OFSI assesses that Garantex has moved its liquidity to Grinex via A7A5. OFSI notes:

- The websites of Garantex and Grinex use a visibly similar interface.
- Some users that lost funds during the Garantex takedown were reimbursed on Grinex.
- Some Garantex clients are moving funds to Grinex.
- Some Grinex users report visiting Garantex's office for account verification.
- Garantex administrators have coordinated the provision of liquidity with Grinex.
- As of May 2025, Grinex's incoming and outgoing transaction volumes exceeded USD 1.2 billion in USDT.
- Grinex accepts payments from Russian DPs.
- Significant volumes of funds have been transferred between Grinex and global licenced exchanges between March and May 2025.

This reformulation is likely to constitute a significant attempt to evade or circumvent sanctions. UK cryptoasset firms should proceed with caution and might want to consider applying a risk-based approach to compliance regarding any transactions involving Grinex addresses.

North Korean cyber activity targeting UK firms

4. It is **highly likely** that UK-based cryptoasset firms are currently at risk of being targeted by DPRK-linked hackers and IT workers seeking to steal or obtain funds through illicit means.

Democratic People's Republic of Korea (DPRK, a.k.a North Korea)-linked threat actors present the most significant and persistent threat to the cryptoassets sector at present. Some DPRK cyber actors and IT workers are known to operate on behalf of the North Korean Government, including entities designated under the UK's DPRK (Sanctions) (EU Exit) Regulations 2019 ("the DPRK Regulations"). The activities described below would breach UK financial sanctions if the activities were designed so that funds or economic resources derived from them were made available to entities or individuals designated (or persons owned and controlled by those directly designated) under the DPRK Regulations.

Cryptoasset heists

UK cryptoasset firms face a severe and persistent threat of having their digital assets stolen by malicious DPRK cyberactors. Actors linked to the DPRK have been responsible for multiple high value cryptoasset thefts globally since 2022, targeting services and users across all jurisdictions. It is likely that hackers associated with the DPRK will continue to attempt to compromise systems and steal assets held at these institutions, including in the UK. The threat of cryptoasset theft applies to both UK firms and individuals operating in the cryptoasset sector.

In February 2025, DPRK-linked actors were responsible for the theft of ~1.5 billion USD in cryptoassets from the exchange Bybit, representing the largest ever cryptoasset exploit.[24] Other confirmed DPRK hacks have targeted exchanges and multiple DeFi companies in various jurisdictions.[25] DPRK-linked threat groups involved in malicious crypto activity include those commonly known as the Lazarus Group, Andariel, BlueNoroff, ScarCruft and Kimsuky, as well as campaigns such as CryptoCore, TraderTraitor, and AppleJeus.

When targeting custodial services, such as centralised exchanges, DPRK actors may seek to compromise private keys of addresses holding customer assets. DPRK actors often make use of social engineering techniques and spread phishing campaigns to inject malware to compromise systems and steal cryptoassets from firms and individuals.

[24] Internet Crime Complaint Center (IC3) | North Korea Responsible for $1.5 Billion Bybit Hack.
[25] For example, see: FBI, DC3, and NPA Identification of North Korean Cyber Actors, Tracked as TraderTraitor, Responsible for Theft of $308 Million USD from Bitcoin.DMM.com — FBI and Treasury Targets DPRK's International Agents and Illicit Cyber Intrusion Group | U.S. Department of the Treasury.

Merlin Dex

In April 2023, a UK-based DeFi project named Merlin Dex was targeted by malicious DPRK cyberactors, who stole 1.8 million USD worth of cryptoassets from the protocol by draining its liquidity pools. The attack was likely a private key compromise or intentional backdoor insertion that granted the deployer - likely a North Korean IT worker - approval to spend tokens held within the project. The stolen funds were bridged back to Ethereum, swapped for Ether (ETH) and transferred to other addresses.

Lykke

In June 2024, the UK based instant exchange platform Lykke was targeted by hackers, leading to the loss of ~ 19.5 million USD. The attack has been attributed to malicious DPRK cyberactors, who stole funds on both the Bitcoin and Ethereum networks. The primary method of laundering assets was through a no-KYC exchange. Funds that were stolen on the Bitcoin blockchain were bridged to the Ethereum network via Thorchain and then deposited into a no-KYC exchange.

Money laundering

DPRK-linked threat actors have both the capability and the intent to target cryptoasset firms to launder illicit funds or economic resources. The DPRK operates some of the most sophisticated money laundering activities in the cryptocurrency space at present. UK cryptoasset firms typically lack the privacy features that DPRK cyber actors prefer, making large-scale exploitation for money laundering purposes unlikely at present. However, many global cryptoasset firms that are currently targeted by DPRK networks have a large UK customer base.

Malicious actors associated with the DPRK employ complex money laundering activities that use multiple types of services and applications. In general, DPRK-linked actors make use of complex money laundering techniques involving a combination of decentralised and centralised exchanges, mixers/tumblers and privacy protocols, bridges, P2P services and highly liquid OTCs in third jurisdictions that offer a greater degree of anonymity to move stolen assets. DPRK-linked actors may seek to clear exposure by off-ramping cryptoassets at centralised exchanges and OTC trading desks, particularly those that operate on the Tron blockchain. DPRK threat actors may also seek to exploit stablecoins, such as USDT and DAI, to allow them to interact with OTC desks in third jurisdictions, where they trade the stablecoins for fiat currency. OFSI notes that DPRK-linked actors have

been known to use highly liquid OTC services based in China, Cambodia and Russia to off-ramp stolen cryptoassets.

OFSI notes that DPRK-associated layering to launder illicit cryptoassets is not linear, and often includes a combination of the following types of services: moving assets through multiple chains, the use of uncommon tokens, chain hopping, bridging, the use of mixers and privacy protocols, the use of numerous intermediary addresses, the use of instant exchange services, asset swapping, and the use of fraudulently obtained or purchased credentials. Based on information available to OFSI, malicious DPRK actors have also been known to create fake exchanges to assist them in laundering cryptoassets. If blockchain analysis firms label an address, or a series of addresses as belonging to an exchange, DPRK money launderers can pass funds to those addresses, and then transfer them onwards, clearing exposure. OFSI also notes that DPRK actors may also seek to exploit newly launched services and applications, particularly in the DeFi space to launder the proceeds of illicit activities, in addition to using common services.

IT Workers

In September 2024, OFSI assessed that UK cryptoasset firms were being targeted by North Korean IT workers disguised as freelance third-country IT workers to generate revenue for the DPRK regime. In an advisory on North Korean IT Workers, OFSI also noted that there was a realistic possibly that IT workers gaining privileged access to sensitive or critical company information could result in this information being compromised or misused by other malign DPRK cyber actors. OFSI has provided detailed information on how DPRK IT workers operate, including by identifying red flag indicators and due diligence measures to help UK firms avoid inadvertently hiring such individuals and to help cryptoasset firms identify such activity abusing their services. UK firms are advised to consult the advisory and report all suspected activity relating to this threat to OFSI as soon as it is identified.[26]

[26] For more information, see OFSI_Advisory_on_North_Korean_IT_Workers.pdf.

Iranian cryptoasset firms with links to DPs

5. It is **likely** that UK cryptoasset firms are currently facilitating transfers to Iranian cryptoasset firms with suspected links to DPs.

Since its legalisation of cryptocurrency mining in 2019 and the subsequent introduction of the digital Rial in 2024, Iran has developed a complex cryptoasset ecosystem. This is likely due in part to international financial sanctions on Iran, including those imposed by the UK, which have contributed to the depreciation of the Iranian Rial and have impacted the Iranian economy. Since 2022, Iran has increased its usage of cryptoassets as payment in foreign trade, including through the prevalent use of USDT, with transactions patterns linked to Iranian centralised exchanges indicating capital flight. This likely reflects an attempt by Iran to leverage cryptoassets as an alternative system to traditional financial services in the context of international sanctions.

According to information available to OFSI, there is a realistic possibility that Iranian cryptoasset firms with suspected links to DPs are presently involved in facilitating payments through the UK cryptoasset infrastructure. The majority of these payments reported to OFSI to date were made to unknown end users using the services of Nobitex, an Iranian cryptoasset exchange with suspected links to the Islamic Revolutionary Guard Corps (IRGC), a designated entity. This activity could amount to a sanctions breach (e.g., if there is no relevant OFSI licence in place).

Certain Iranian-linked cryptoasset platforms have also provided public guidance to users on methods to circumvent international financial sanctions imposed on Iran. This includes advice on social media sites on how to move funds in and out of Iran using cryptoassets to bypass traditional banking restrictions. OFSI notes that certain Iranian platforms have been linked to offering Artificial Intelligence-generated identification for customers to bypass KYC checks usually required by compliant cryptoasset exchanges. UK firms should report to OFSI any suspected activity involving Iranian DPs or Iranian cryptoasset firms suspected to be facilitating UK financial sanctions evasion or circumvention as soon as it is discovered.

Intermediary jurisdictions

Jurisdictions with rapidly growing and legitimate crypto markets may be exploited by criminals and actors seeking to launder the proceeds of illicit activity. It is important that these jurisdictions have regulations in place to ensure compliance with international standards on cryptoassets and respond to emerging threats. OFSI works closely with the relevant authorities in these intermediary jurisdictions.

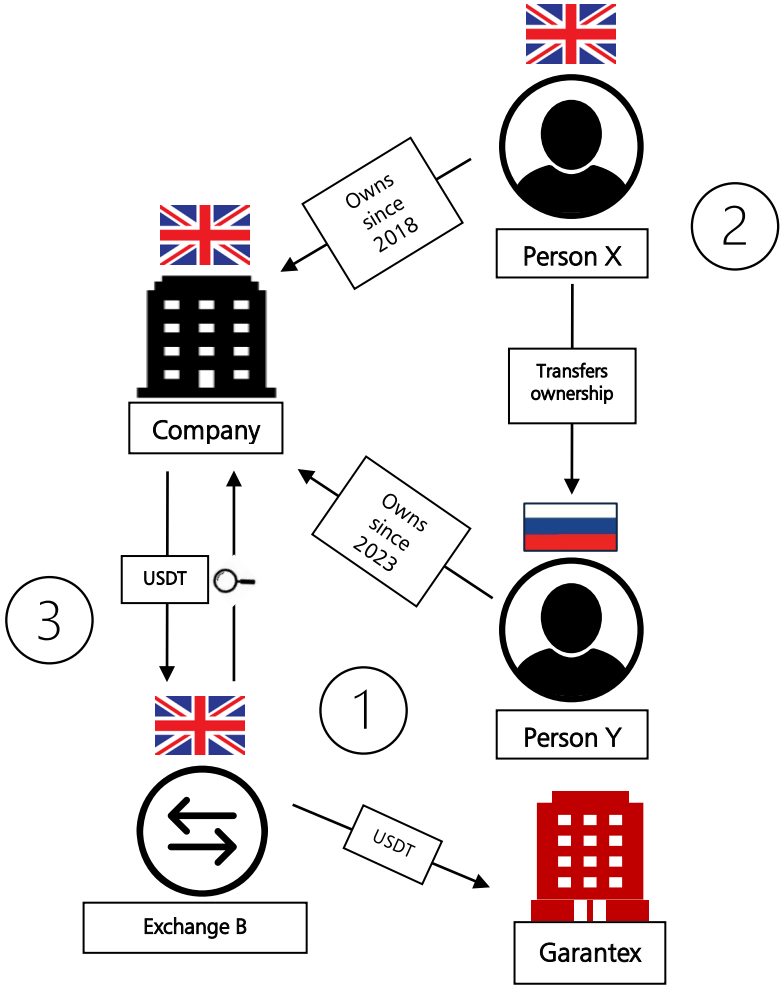
CASE STUDY 1: Direct Exposure to a Sanctioned Entity

1. A UK company, Company A, sends a significant amount of USDT to GARANTEX, a Russian DP since 2023, via their account held with a UK cryptoassets firm, Exchange B.

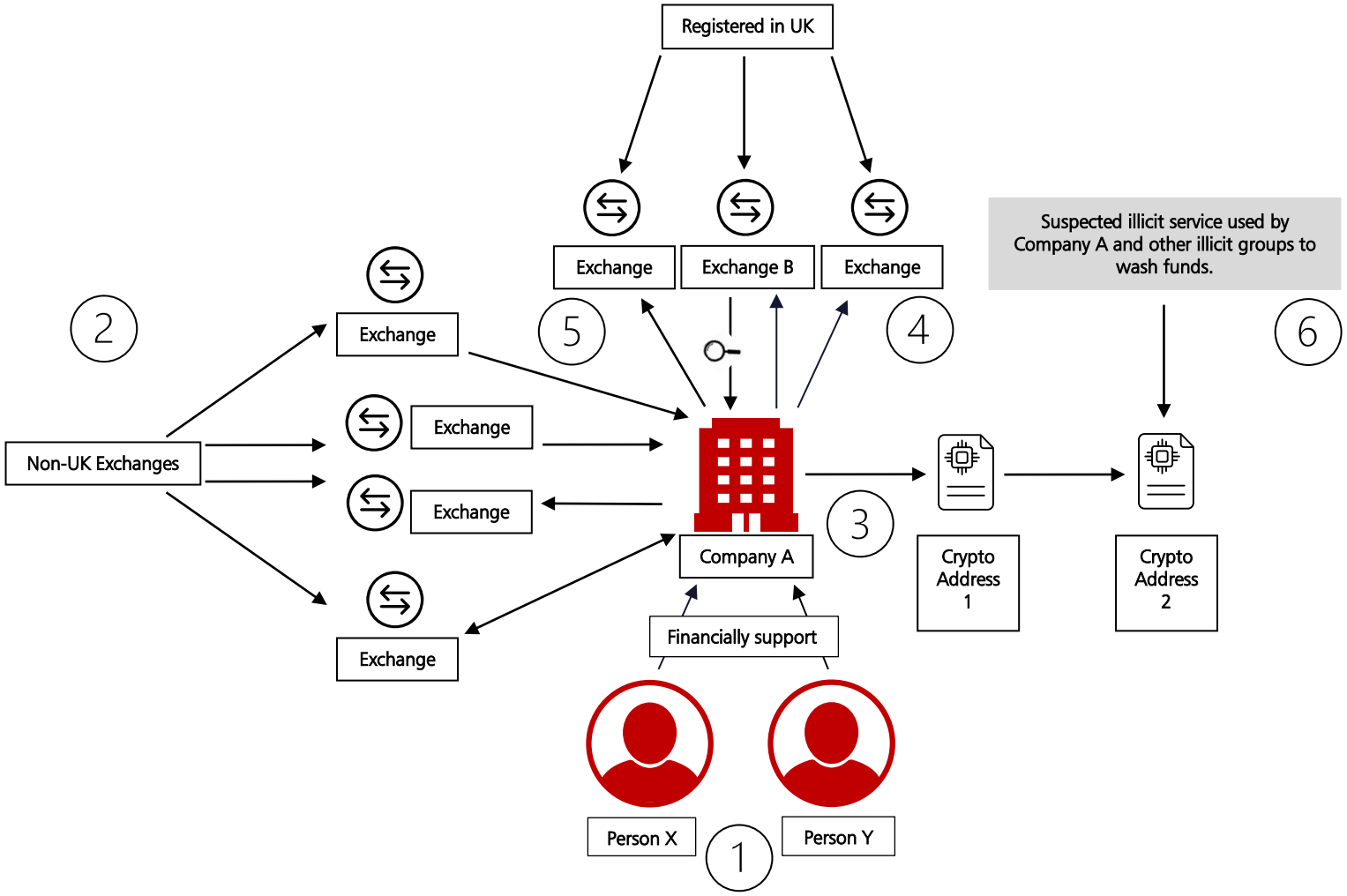
2. Know-Your-Customer details obtained by Exchange B match those of a UK national, Person X, who was the owner and director of Company A when the company was established, until they transferred control to a Russian national, Person Y.

3. The transaction is indicative of a sanctions breach under the Russia (Sanctions) (EU Exit) Regulations 2019 ("the Russia Regulations").

Exchange B must submit a Compliance Reporting Form to OFSI and also report to the FCA and the NCA via the usual reporting mechanisms.



CASE STUDY 2: Darknet Services



1. Person X, a British national, and Person Y, a foreign national, are designated by the UK Government for their involvement in providing financial support to Company A, an entity designated by the UK. Both individuals are subject to asset freezes. As part of the designation, several crypto addresses owned or controlled by Persons X and Y and Company A, also become subject to the asset freeze.

2. Several of these deposit addresses are held at large non-UK centralised cryptocurrency exchanges. Once they are frozen, the addresses held at compliant centralised exchanges are no longer available to Persons X and Y and Company A.

3. Other addresses are held independently by Company A. They can still be used by the DPs, in breach of sanctions.

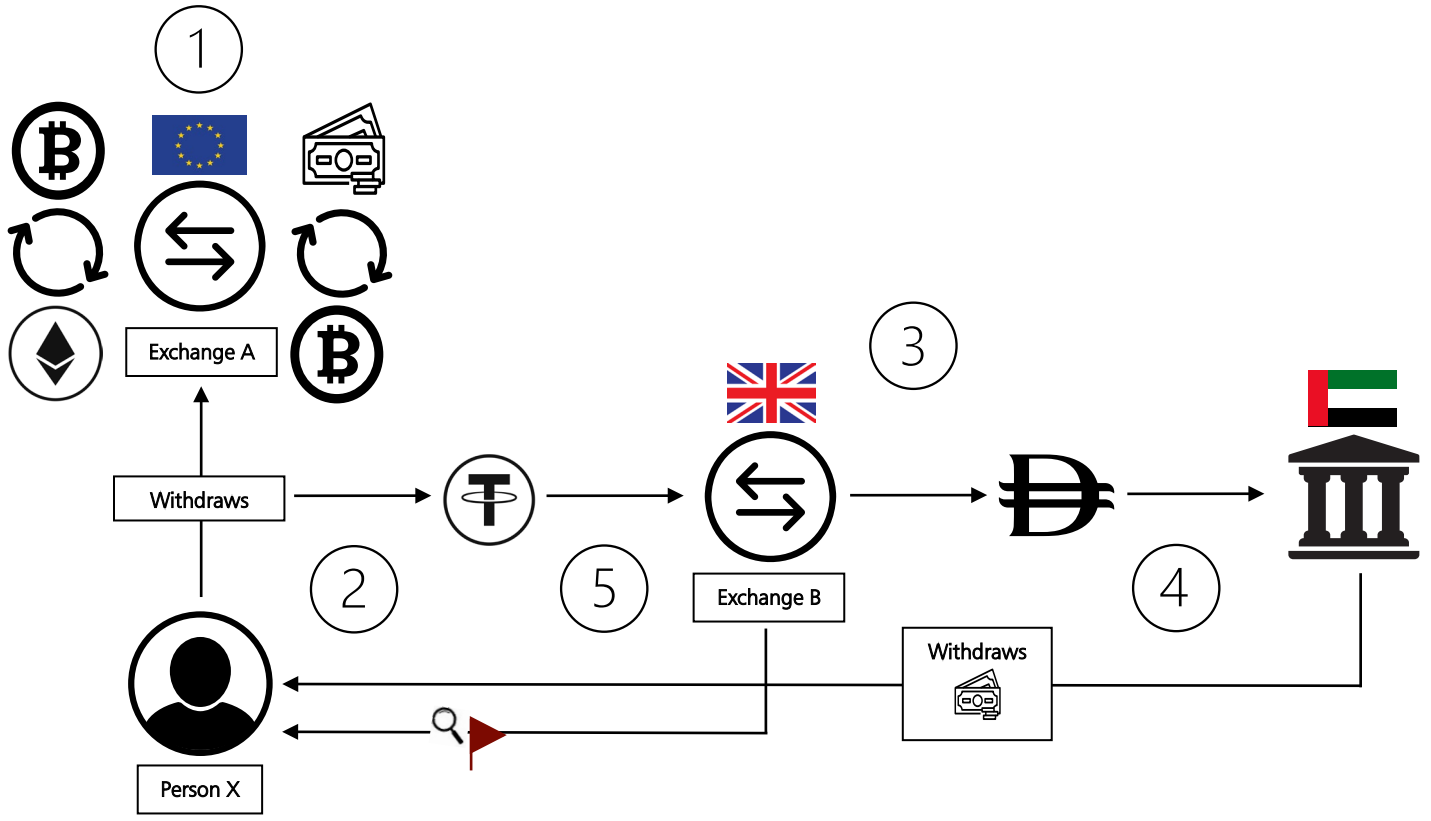
4. After the designation, Persons X and Y continue making crypto transactions involving the Company A listed addresses to the addresses previously used and several new addresses, likely created following designation. Company A also continues to deposit funds at various crypto exchanges registered in the UK, including Exchange B.

5. Using blockchain analytics, Exchange B links one of the wallets controlled by Company A to a suspected laundering service. As cryptoassets held in frozen wallets by compliant centralised exchanges are unavailable, using illicit laundering networks is a way for the DPs to bring the assets back into circulation and to disguise the fact that the funds originated from a designated entity.

6. Some of these transactions are likely to be indicative of sanctions breaches. They are also indicative of how DPs can exploit darknet services traditionally associated with Organised Crime Groups to evade sanctions and launder cryptoassets.

As a relevant firm as defined in UK legislation, Exchange B must submit a Compliance Reporting Form to OFSI, as well as a SAR to the NCA, to report the suspected illicit activity.

CASE STUDY 3: Exchanges of Fiat into Cryptocurrency



1. Exchange A is a European cryptoasset firm that facilitates both crypto-to-crypto and crypto-to-fiat exchanges.

2. Person X, a non-UK individual, uses Exchange A to withdraw a significant amount of Russian Ruble from a Russian bank designated by the UK under the Russia Regulations and exchange them into the stablecoin USDT.

3. Once the cryptoassets are withdrawn, Person X proceeds to convert the USDT into United Arab Emirates (UAE) Dirham using the services of another large UK cryptoasset firm, Exchange B.

4. Person X then withdraws the money though a UAE bank account.

5. Exchange B conducts due diligence and identifies the suspicious transaction. It concludes that it is indicative of a sanctions breach.

Exchange B must submit a Compliance Reporting Form to OFSI. Exchange B should also offboard Person X as a customer in line with its risk-based approach to compliance.

Further resources

This assessment highlights OFSI's ongoing commitment to proactively engage with stakeholders to ensure UK financial sanctions are properly understood, implemented, and enforced in the UK. This report is the last in a series of sector-specific threat assessments published by OFSI in 2025.[27] OFSI has also published, and will also continue to do so, information on specific threats to UK financial sanctions compliance, including, for example, the recent advisory on North Korean IT workers (available here).

This assessment does not represent legal advice and should be read in conjunction with OFSI guidance (available here). OFSI encourages cryptoasset firms to review the Frequently Asked Questions (FAQs) published by OFSI which provide short form guidance and technical information on financial sanctions (available here). OFSI also encourages all UK firms to subscribe to free OFSI e-mail alerts (available here) to receive further relevant information about UK financial sanctions.

This assessment builds on previous and related publications issued by OFSI and UK Government partners, including four previous threat assessment reports published by OFSI in 2025 (available here), the Red Alert on Financial Sanctions Evasion Typologies By Russian Elites and Enablers published by OFSI and the NCA in July 2022 (available here), the Red Alert on Shadow Fleet Sanctions Evasion and Avoidance Network published by OFSI and the NCA in July 2025 (available here), and the National Risk Assessment of Money Laundering and Terrorist Financing 2025 (available here). OFSI also encourages UK cryptoasset firms to review publications from other relevant UK Government bodies, including the NCA, the FCA and the PRA.

[27] OFSI Threat Assessment Reports - GOV.UK.



Office of Financial
Sanctions Implementation
HM Treasury