Rahapesu Andmebüroo

Sanctions evasion through the use of virtual currencies

24 June 2023

Executive summary

The three general typologies used to evade sanctions using virtual currencies are: the **direct *or peer-to-peer* model**, the **intermediary model** and the **escrow model**. The review describes the three models mentioned and highlights indicators that allude to a heightened risk of evasion. The risk indicators for sanctions evasion have been selected based on both Estonian and international practice. The review ends with the main factors for ensuring compliance checks to mitigate the risks.

Typologies of sanctions evasion

Direct or peer-to-peer model

Direct or peer-to-peer virtual currency transactions between different parties are the most immediate way to move funds in a simple way (Figure 1). Although direct entries between crypto asset addresses are technically the simplest method, this is sufficient to enable discrete business operations. Consequently, the peer-to-peer model is also one of the most widely used methods of sanctions evasion, especially for one-off transactions of any amount.

Figure 1. Direct or peer-to-peer model

Intermediary model

The intermediary model is a more sophisticated virtual currency trading system in which crypto assets are purchased, concealed, invested, traded and sold through a specific network of business contacts, which includes, for example, entrepreneurs, virtual currency service platforms and companies that sometimes have state participation.

One of the most important components of the intermediary model is a reliable partner who is prepared to be involved in the sanctions evasion. Such a partner may be, for example, a country outside the European Union where sanctions against Russia are not adhered to. Such a pattern of behaviour emerged when, shortly after Russia's aggression began, billion-dollar portfolios of virtual currency were moved out of the European Union and other jurisdictions imposing sanctions on Russia to third countries. For example, virtual currency service providers in the United Arab Emirates (UAE) were among the first recipients and transferors of virtual assets portfolios of Russian and Belarusian citizens.

The intermediary model consists of several layers of intermediaries, through which significant amounts of Russian-related funds and virtual currencies are moved. The first link in this model is the country subject to sanctions, in this case Russia, where the state itself and state-owned companies or persons linked to the state have assets in local currency, ie rubles, to a considerable extent. As a next step, banks linked to Russia or the central bank will be ordered to transfer funds to the correspondent banks in non-sanctioned and Russia-friendly countries (eg UAE) (Figure 2).

The correspondent bank exchanges the local currency of the sanctioned country into, for example, US dollars or euros, and then transfers these funds to intermediaries in third countries, ie persons operating in reputable or low-profile companies. This layer of intermediaries converts money into virtual currency and moves it through multiple crypto asset

addresses to hide the true origin of the funds and ensure anonymity. The virtual currency is then converted back into a fiat currency (eg the US dollar) and returned to the bank of a sanctioned country via correspondent banks, or partially left in virtual currency for other purposes (eg for transactions and trading, or redirected to state-linked crypto asset addresses for further investments).

The intermediary model makes it possible to organise trade at the state level and transactions with larger amounts. At the state level, this model in particular has been actively used by North Korea.

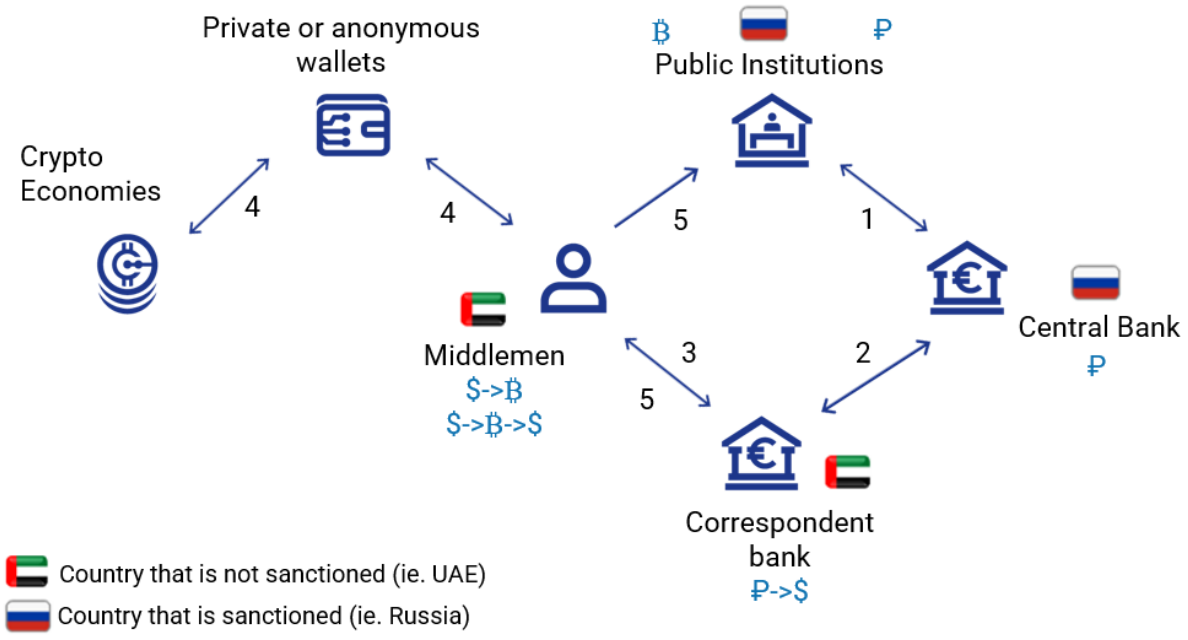

Figure 2. Intermediary model

Escrow model

The escrow model can be viewed as an automated, anonymous and smaller-scale variant of the intermediary model. Escrow is a market environment that automatically matches anonymous buyers and sellers. Transactions on the market are organised by an escrow system intermediary who ensures the security of trading (Figure 3).

Trading conditions are defined in a previously coded script or smart contract. This kind of trade in goods and services is automated — the transaction takes place when the buyer and seller fulfil the conditions specified in the escrow system. If one of the parties or both parties fail to comply with the predefined conditions, the funds deposited for the transaction will be returned to the buyer and the seller and the transaction will not take place.

This escrow system has been actively used by Sberbank operating in Russia in the provision of real estate transaction services. The system can also be successfully used when exchanging many other goods and services for virtual currencies. However, the success of such transactions depends on the intermediary providing the escrow service, who may also be subject to sanctions or impose rules on sellers and buyers on the market according to risk appeals.

Figure 3. Escrow model

Risk indicators of sanctions evasion

The following are the most common risk indicators for evasion, which can be observed in all three of the above sanctions evasion models.

The customer's portfolio consists **solely of privacy coins** or the value of the privacy coins in the portfolio makes up a large share of the customer's **total assets.**	Active use of privacy coins may indicate an intention to hide the origin of the assets and the movement of funds to prevent the identification of a person included in the sanctions list.
The **customer will not or cannot provide information** about the **origin of privacy coins** that are or have been in their portfolio.	Privacy coins may originate from a person in the sanctions list or relate to transactions with sanctioned goods.
The customer provides **inaccurate or incomplete information when opening an account**. The customer does not respond to queries or **refuses to update** the information required for the implementation of the measures of the 'Know your customer' policy.	Collecting personal identification information helps to exclude the possibility that the customer is a person included in the sanctions list and their refusal to provide information refers to an attempt to conceal their identity.
The customer does not respond to a request made by the provider of the virtual currency service or **refuses** to provide additional information about **transactions on the account.**	The desire to hide the circumstances of the transaction may indicate that a party to the transaction is included in the sanctions list or the transaction may be linked to sanctioned goods.

Crypto asset addresses are listed in important **checklists**, such as the lists of the U.S. Department of the Treasury's Office of Foreign Assets Controls (OFAC) or law enforcement.	So-called blacklisted addresses are more likely to relate to persons included in the sanctions list. The imposition of a sanction to persons included in the OFAC list is not a legal obligation in Estonia, however the parties included in the list are related to a higher risks and may also have direct links to EU-sanctioned parties.
Several customers sign up over a **short period of time** using the **same address, mobile device, telephone number, IP address** etc.	A person or company added to the sanctions list may create different accounts from the same location and move smaller amounts through multiple users to conceal their identity.
The customer attempts to **log on** to the virtual currency service platform using an **IP address** or **VPN** associated **with a sanctioned jurisdiction.**	Logging into one's account from a sanctioned jurisdiction and using a VPN indicates a heightened risk of evasion or violation of sanctions.
The virtual currency service platform receives **unusual or frequent queries** about the **customer's funds from other providers**.	Such queries refer to a customer's higher level of risk; the customer or the virtual currency owned by the customer may be subject to sanctions.
Transfers to multiple addresses. The purpose of the transactions appears to be to conceal the origin of the asset or the planned use of funds.	A person included in the sanctions list may intentionally attempt to conceal the origin of the asset and make it difficult to monitor the movement of funds within the blockchain.
Customer transactions take place **at the same time of day**. Transfers are made by exchanging fiat currency for virtual currency and then exchanging virtual currency back to fiat currency.	Such a pattern of transactions suggests that the customer has thought the use of the model through and it may have been designed to conceal the origin of the assets and make it difficult to track the movement of funds within the blockchain.
The customer receives virtual currencies from an OTC address by making several quick transactions between different virtual currencies (exchanging one virtual currency for another) immediately upon receipt, followed by a transaction where the funds are transferred from the virtual currency service platform to another address.	Such activity may refer to an attempt by a person included in the sanctions list to conceal the origin of the assets and make it difficult to monitor the movement of funds within the blockchain. Less advanced blockchain analysis software detects, on average, only the last four transactions or operations that were done with a specific virtual currency.

Large volume of transfers and frequent transactions between different types of virtual currencies.	Moving larger amounts indicates a higher risk of sanctions evasion, while transacting in different virtual currencies may indicate an attempt to conceal the origin of assets and make it difficult to monitor the movement of funds within the blockchain.
When registering an account on the virtual currency service platform, the customer provides an **anonymous email address** that originates from an **encrypted email service.**	The use of an encrypted email address is unusual among ordinary customers and refers to the customer's desire to remain anonymous, resulting in a higher risk of sanctions evasion.
Funds or virtual currencies are moved (added or withdrawn) to an address with direct or indirect links to suspicious sources that have been identified during the blockchain analysis, including, for example, **dark web**, ***mixing/tumbling*** **services** and **ransom/cybercrime**.	The association of a crypto asset-address with the suspicious sources mentioned increases the risk that there may be a company or person who uses suspicious sources to conceal their activities and identity behind the transactions.
Before reaching the customer's address or immediately after withdrawing funds from there, the **virtual currency moves through a large number of different addresses in a very short period of time.**	Rapid movement of virtual currency through many addresses makes it more difficult to identify the origin of financial assets. A person included in the sanctions list who wishes to conceal their identity may be behind such transactions.
Virtual currency goes through ***mixing/tumbling*** **services** and is transferred to several addresses where the virtual currency is exchanged for fiat	The use of such services indicates the desire to hide the origin of funds and make it difficult to monitor the movement of funds within the blockchain.
The virtual currency originates from an OTC virtual currency service provider, which advertises its services as private and anonymous.	It is more likely that a service provider who focuses on ensuring anonymity is selected for sanctions evasion.
The crypto asset address has been mentioned on a **crowdfunding platform or social media** in relation to a call **to support Russian military action** or any other **country subject to sanctions**.	A connection to such websites is one of the clearest indications of a sanctions violation. In most cases, the participants are private individuals who directly support Russia's military action in Ukraine.

The origin of the **assets** used to purchase virtual currency is unknown.	Lack of information about the origin of the assets significantly raises the risk of sanctions evasion, especially if it is also a transaction of high monetary value.
The customer often receives **transfers from several payment institutions** who are located in a high-risk jurisdiction and/or whose **'Know your customer' policy measures** and **identification procedures** may be **less stringent** than average. The customer uses **such payment institutions** when making transfers.	Individuals included in the sanctions list prefer to use payment institutions to transfer funds to a virtual currency service provider, since their 'Know your customer' policy measures are generally considerably less stringent compared to traditional banks.
Customer transactions are initiated or sent from **IP addresses** that point to a location in **Russia, Belarus** and, in the context of the Financial Action Task Force (**FATF**), a **jurisdiction with incomplete measures**, a sanctioned jurisdiction. The IP address may also have been flagged as suspicious.	Transactions originating from such jurisdictions are related to higher risk and are more likely to involve evasion and infringement of sanctions.

In addition to the above risk indicators, virtual currency service providers should also pay close attention to the **dangers posed by North Korean cybercrime**, which has become increasingly relevant in recent years. According to a UN report, damage caused by North Korean cybercrime was record-breaking in 2022, more specifically the country received nearly four billion dollars worth of virtual currencies as a result of cybercrime. North Korea is known to use funds derived from cybercrime to fund its nuclear program. Often, North Korean hackers take advantage of vulnerabilities of platforms offering a virtual currency service by selecting service providers that fail to implement appropriate security measures in depositing customers' assets.

Key factors to ensure effective compliance checks

Management support for the compliance check system

The management's commitment to compliance with sanctions is one of the key factors in the successful functioning of the compliance check system. Management support is important as it helps to ensure that the sanctions compliance system receives sufficient resources and is adequately integrated into the day-to-day operations of the company. Public support from the management promotes the use of the compliance check system, motivates the staff to comply with sanctions and promotes a culture of compliance control throughout the organisation.

System testing and auditing

In order to ensure the reliability and effectiveness of the sanctions compliance check system, the system must be tested regularly. For this purpose, a broad and objective method of testing or auditing should be used to assess the functioning of the system to ascertain which aspects need improvement, taking into account the ever-changing risk level and the environment of sanctions.

Depending on the size of the company and the complexity of the activity, the conformity of the sanctions compliance system must be audited either internally or by involving external auditors in the audit process.

Risk assessment and internal rules of procedure

Risk assessment and internal rules of procedure that ensure compliance with the conditions laid down by law will help to protect against accidental business activities with persons included in the sanctions list. Risk assessment must be tailored to a specific company, taking into account their customer base, partners, products and services, supply chain, area of operation, and direct and indirect points of contact with other jurisdictions and potential sanctioned persons. When assessing risks, it may be necessary to assess whether the transaction partners have adequate compliance control mechanisms.

Internal rules of procedure must be based on risk analysis. Effective rules of procedure help to apply due diligence measures and identify potential risk factors. Internal rules of procedure often involve the use of industry-specific tools, including for screening, monitoring and further investigation of transactions. The ‘Know your customer’ policy measures must be applied both at the beginning of the customer relationship and throughout the business activity to identify persons who may attempt to conceal the origin, owners or actual beneficiaries of the asset.

Training of employees

A training programme for employees focusing on sanctions is one of the most important components for the functioning of the company's sanctions compliance system, as it enables to ensure timely detection of a sanctions breach. The content and scope of the internal training programme must be determined based on the size of the particular enterprise, the complexity of its activities and the risk assessment. The training programme must correspond to the company's specific characteristics, ie take into account the products, services, customers, partners and area of activity offered, and be in accordance with the principle of proportionality. A well-developed training programme takes into account the needs of a particular position. Such training will ensure that the employees of the company are informed of the specific area of responsibility for the application of sanctions and that the company as a whole can ensure effective compliance with sanctions.

Sources

FINTRAC, Money laundering and terrorist financing indicators — Virtual currency transactions, June 2021, https://fintrac-canafe.canada.ca/guidance-directives/transaction-operation/indicators-indicateurs/vc_mltf-eng#s1
FinCen, FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts), March 7, 2022, https://www.fincen.gov/news/news-releases/fincen-advises-increased-vigilance-potential-russian-sanctions-evasion-attempts
OFAC, Sanctions compliance guidance for the virtual currency industry, October 2021, https://ofac.treasury.gov/media/913571/download?inline
SUERF, Is it easy to hide money in the crypto economy? The case of Russia, SUERF Policy Brief, No 506, Jan 2023, https://www.suerf.org/suer-policy-brief/59935/is-it-easy-to-hide-money-in-the-crypto-economy-the-case-of-russia
United Nations, Panel of Experts established pursuant to Security Council resolution 1874, June 2022, https://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/N2225209.pdf