Observations related to sanctions evasion

Introduction

This document, published in connection with the summary of the sanctions risk assessment, collates information obtained through cooperation between authorities and from reliable public sources on identified ways of evading sanctions. The purpose of the appendix is to provide supervised entities with information they can utilise when preparing their own policies and procedures to prevent sanctions evasion.

Sanctions evasion usually refers to participating knowingly and intentionally in activities that have the object or effect of evading prohibitions[1] under sanctions regulations, including participating in such activities without deliberately seeking that object or effect, but being aware that the participation may have that object or effect and accepting that possibility.

In practice, this may mean activities aimed at, for example, avoiding the freezing of assets by creating complex chains of ownership that obscure the actual beneficiary that is subject to sanctions. Moreover, transporting sanctioned goods to a third country[2], knowing that the goods will be forwarded to a sanctioned country, may also be considered as sanctions evasion.

Russia, Belarus, the Democratic People's Republic of Korea ("North Korea") and Iran in particular, are countries with which a high risk of sanctions evasion is associated and which have been found to have actively evading sanctions. There is also a heightened risk of sanctions evasion associated with neighbouring countries of the aforementioned jurisdictions and it is possible that attempts could be made to circumvent sanctions also through these neighbouring countries. For example, in its 2014 report on Iran, the UN Panel of Experts found that the country was attempting to utilise companies registered in neighbouring countries to evade the export sanctions imposed on it[3]. With regard to sanctions against Russia, sanctions evasion has also been observed in, for example, Finland[4] and other neighbouring countries of Russia.

Threat of sanctions evasion related to state actors

Russia

From a sanctions perspective, a significant threat to the Finnish financial sector relates to sanctions against Russia (hereinafter "Russia sanctions") and their evasion. Russia's actions are planned, organised and very wide-ranging. The parties involved in sanctions evasion are also highly adaptable, which creates additional challenges in detecting and preventing sanctions evasion.

The illegal war of aggression launched by Russia in Ukraine in February 2022, and the significant losses of equipment it has experienced there, have forced Russia to acquire new military equipment to replace what it has lost in the battlefield. As a result, Russia has had to rely on, among other things, components and advanced technology

[1] See, for example, Council Regulation (EU) 269/2014, Article 9.

[2] Third country refers to a state that has not imposed sanctions on the target country (e.g. Russia) and thus the state in question does not, moreover, monitor compliance with the sanctions in question.

[3] UN Panel of Experts 5 Jun 2014 p. 26, http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/S_2014_394.pdf

[4] Two years of war in Ukraine - Customs has opened more than 740 criminal investigations into sanctions violations, Customs 21 February 2024 (in Finnish), https://tulli.fi/-/kaksi-vuotta-ukrainan-sotaa-tulli-on-aloittanut-yli-740-esitutkintaa-pakotteiden-rikkomiseen-liittyen/

manufactured by Western companies to maintain and modernise its military machine. At the same time, however, extensive sectoral sanctions have been imposed on Russia, and key products for Russia's military industry have been placed under export bans. These measures have adversely impacted and slowed down the renewal of weapons and equipment. Russia has sought to respond to the difficult situation caused by sanctions by actively using various procurement networks to transport sanctioned products and items to Russia[5]. In addition, it has stepped up cooperation with Iran and North Korea to acquire, among other things, unmanned aerial vehicles (drones) and ammunition.

The procurement networks used by Russia are often complex structures whose purpose is to try to obscure information about the end users and intended use of the products. Russia utilises shell and front companies to make acquisitions look like normal transactions. Third countries also play a very important role in circumventing sanctions, as they can act as a transit countries for the transport of sanctioned goods to Russia.

Procurement chains are often long and their specific purpose is to conceal the link to Russia and Russian actors. There is a diverse group of different actors in the procurement networks, some of which may have links to the Russian security services, others to organised crime[6], and in addition there may be actors who primarily seek to benefit financially from the opportunity offered by the situation. A procurement network may also include actors that are unknowingly involved in activities and may not be aware that they are being used as part of the Russian military machine's procurement network.

Procurement networks linked to Russia have also operated in Finland. For example, the CEO of two Finnish companies received a nine-month suspended sentence for regulatory breaches and criminal export of defence materiel[7]. The verdict has been appealed to the Court of Appeal. The case concerned, among other things, the export of tools subject to export restrictions from Germany to Russia in such a way that the products had been reported to Finnish Customs as being exported to Kazakhstan. However, material found in the company's computer systems showed that the goods had gone to St Petersburg.

In its sanctions evasion activities, Russia has used third countries that have not imposed sanctions on Russia as a result of the illegal war of aggression it started in Ukraine. Russia has circumvented sanctions, notably via Central Asian states[8], China, Hong Kong, Turkey and the United Arab Emirates (UAE).

An emerging threat related to Russia sanctions is virtual currencies. There are indications that Russian procurement networks have also used virtual currencies to circumvent sanctions. For example, large Russian banks have started to offer their customers the possibility to trade abroad in virtual currencies[9]. In addition, sanctions imposed by G7 countries[10] have allegedly been circumvented through Russian virtual currency exchange service providers[11].

[5] " Threats to national security", Finnish Security and Intelligence Service https://supo.fi/en/threats-to-national-security [referenced 31 May 2024]

[6] Europol (2023), European Financial and Economic Crime Threat Assessment 2023 - The Other Side of the Coin: An Analysis of Financial and Economic Crime, Publications Office of the European Union, Luxembourg, p. 8

[7] Itä-Uusimaa District Court R 24/287. The District Court's judgment has been appealed to the Court of Appeal.

[8] Kyrgyzstan, Kazakhstan, Turkmenistan, Tajikistan and Uzbekistan

[9] "Treasury Designates Russian Companies Supporting Sanctions Evasion Through Virtual Asset Services and Technology Procurement" Office for Foreign Assets Control (OFAC) 25 Mar 2024, https://home.treasury.gov/news/press-releases/jy2204

[10] Sanctions have been imposed by the EU, the United States, the United Kingdom, Canada and Japan.

[11] "US, UK Probe $20 Billion of Crypto Transfers to Russian Exchange" Bloomberg 28 Mar 2024, https://www.bloomberg.com/news/articles/2024-03-28/crypto-transfers-to-russian-exchange-worth-20-billion-probed-by-us-uk

Phenomenon: Procurement from Finland of products subject to sanctions and their export directly or via third countries to Russia

Russia actively seeks to obtain from Western countries the sanctioned goods it needs, particularly to maintain the operational capacity of its military machine. Products are also procured from Finland or ordered and transported from abroad to Finland, from where they are exported either directly or via third countries to Russia.

Sanctioned items include various products related to electronics, computers, sensors, navigation and aviation. In addition, luxury goods, for which there is still demand in Russia, are subject to sanctions. Exports of the above products to Russia are prohibited under EU sectoral sanctions regulations.

Sanctioned products may be acquired directly from the manufacturer of the product, particularly in the case of products intended for industrial use. Front companies and third countries may be used to conceal the link to Russia.

In addition, consumer products such as computers, smartphones and drones are purchased from Finnish online stores, among others. Credit cards issued by foreign (and particularly third country) banks may be used for the purchases and the names used in the orders may be fictitious.

Typically, the Finnish party who is manufacturing, selling, brokering or transporting sanctioned goods is not aware that the end-user of the goods is in Russia. Nevertheless, it would be important to be able to detect possible anomalies associated with such transactions in order to prevent as effectively as possible sanctioned goods ending up in Russia.

To ensure the effective implementation of sanctions, it is important that financial sector actors are vigilant against attempts to circumvent export bans and sectoral sanctions imposed on Russia.

Examples of sectors that may be at heightened risk of sanctions evasion:

- technology companies (e.g. companies that manufacture dual-use products)
- logistics companies (e.g. transport and freight, warehousing, forwarding) that have business or trading partners in Eastern Europe, Central Asia or Russia.
- online stores that sell, among other things, consumer products such as computers, mobile phones and drones as well as products related to hiking and hunting.

Examples of actions to manage risks related to sanctions evasion:

- preparing a sanctions risk assessment and keeping it up to date
- taking sanctions into account in customer due diligence processes and risk classification
- taking sanctions into account in correspondent banking relationships (particularly third countries that do not comply with EU sanctions)
- ensuring that the lists used in sanctions screening are up to date

Entities supervised by the FIN-FSA must report to the Finnish Financial Intelligence Unit of any attempts to circumvent sanctions.

Belarus

As a close partner of Russia, Belarus has also played an important role in circumventing the sanctions imposed on Russia, and is an important transit country in exports to Russia of sanctioned goods. Sanctions against Belarus have been imposed long before the Russian invasion of Ukraine.

Belarus has been subject to sanctions since the 2006 presidential elections, which were found to be fraudulent. Sanctions were tightened in 2020 due to violently suppressed demonstrations, which also originated from presidential elections that were found to be fraudulent. Sanctions on Belarus were increased after the country supported Russia's invasion of Ukraine. So far, however, the sanctions have not reached the Russian level in scope, although four Belarusian banks, for example, have been excluded from the Swift messaging system. In particular, export bans on goods have so far been much more limited than those imposed on Russia.

The more limited sanctions imposed on Belarus have created an opportunity for Russia to use Belarus as a transit country to circumvent certain Russian export restrictions.

North Korea

The Democratic People's Republic of Korea, i.e. North Korea, has been subject to very extensive sanctions since the early 2000s, and their purpose is to prevent the advance of North Korea's nuclear weapons programme. North Korea has also consistently sought to circumvent the UN and EU sanctions imposed on it. Russia's recent decision to veto the mandate renewal[12] of the UN Security Council's Panel of Experts will undermine the effectiveness of the sanctions imposed on North Korea. The Panel of Experts has played a key role in monitoring compliance with sanctions. In the absence of monitoring, there is a risk that more parties will enter into transactions with North Korea. Russia, among others, has been found to have sold crude oil to North Korea in violation of UN sanctions[13].

North Korea needs technology manufactured in Western countries to advance its nuclear weapons programme. Finnish companies manufacturing and selling dual-use and other high technology products may therefore also be of interest to North Korea, although no such activity has been observed.

In recent years, North Korea has also carried out an increasing number of cyber attacks against virtual currency providers and financial institutions. Through this activity, North Korea is estimated to have stolen assets worth around USD 1.7 billion[14] in 2022 alone. The stolen assets have been laundered in complex money laundering operations using numerous different crypto service providers and crypto wallets to disguise the origin of the assets. There is a risk that stolen crypto assets can also be laundered through Finnish crypto asset service providers.

Cyber attacks are also a threat to Finnish companies, and it is possible that attacks may target Finland[15]. Furthermore, for example in ransomware-related cases, it should be noted that making so-called ransom payments may violate sanctions if the activity involves parties or countries subject to sanctions, such as North Korea.

[12] "Russia blocks renewal of North Korea sanctions monitors", Reuters 28 Mar 2024, https://www.reuters.com/world/russia-blocks-renewal-north-korea-sanctions-monitors-2024-03-28/

[13] Exclusive: Russia is shipping oil to North Korea above UN mandated levels - US official, Reuters 7 May 2024, https://www.reuters.com/business/energy/russia-is-shipping-oil-north-korea-above-un-mandated-levels-us-official-2024-05-02/

[14] 2024 National Proliferation Financing Risk Assessment p. 5, https://home.treasury.gov/system/files/136/2024-National-Proliferation-Financing-Risk-Assessment.pdf

[15] Sophistication, scope, and scale: Digital threats from East Asia increase in breadth and effectiveness, Microsoft September 2023, https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW1aFyW

Iran

Iran has been subject to extensive UN sanctions because of its nuclear weapons programme. However, sanctions were largely lifted in 2015, when UN Security Council members, led by the US and Russia, persuaded Iran to halt the programme[16].

Iran has also been subject to sanctions for other reasons. The EU has imposed sanctions on Iran after it supplied unmanned aerial vehicles (drones) to the Russian army. Russia has used these drones in Ukraine. Iran seeks to obtain components for the production of drones from Western countries by using complex procurement networks and by concealing the intended use of the products and the country of destination. In addition, Iran has been subject to sanctions because of serious human rights violations by the regime[17].

Iran has been subject to extensive sanctions for decades, which has enabled it to accumulate a wealth of experience and know-how in the various means of evading sanctions. Iran, among other things, utilises front and shell companies that it has established, particularly in the United Arab Emirates and Turkey, thereby attempting to conceal links to Iran itself. Iran also circumvents sanctions by mining bitcoins, which has given it access to a considerable amount of virtual currency[18].

[16] UN Security Council Resolution 2231 https://www.un.org/securitycouncil/content/2231/background

[17] See Council Regulation (EU) 359/2011

[18] "Iran uses crypto mining to lessen impact of sanctions, study finds", Reuters 21 May 2021, https://www.reuters.com/technology/iran-uses-crypto-mining-lessen-impact-sanctions-study-finds-2021-05-21/ (referenced 22.8.2024)