AML & The Impact of the war in Ukraine

by Henry Duggan & Andrew Pimlott

On February 24, 2022, Russia launched an invasion of Ukraine. This unilateral action subsequently resulted in a swath of economic sanctions aimed at Russia from western states aimed at financial institutions, individuals, businesses and other areas. Their objective was to impose economic restrictions on Russia for its aggressive stance in attempting to impose military control over Ukraine.

The actions of Russia had far-reaching implications for the socioeconomic profile of Europe and the global geopolitical landscape. The sanctions were significant and far-reaching. Some examples of these include the following:

- Removing access to the Society for Worldwide Interbank Financial Telecommunication ("SWIFT") global messaging system for some Russian banks[1].
- Restrictions on Russia's ability to access financial services and capital markets[2].
- Sanctions aimed towards specific Russian oligarchs and senior political figures, with assets frozen in a number of different jurisdictions. For example, on April 14, 2022, the Government of the United Kingdom indicated that it had frozen assets of Russian oligarchs up to GBP£10 billion[3].
- Implementing specific deposit limits with EU and UK banks for Russian individuals and businesses[4] [5].

As a result of the dramatic increase in sanctions activity over a relatively short period of time, the risk for financial institutions has risen significantly and may become increasingly more volatile moving forward. Organisations have had to divert time and resources to ensure compliance with these new changes to the international sanction's regime. They have had to ensure that, not only are the intricacies of these new amendments fully understood, but that appropriate changes to policies, procedures, mitigating controls, and technology screening solutions are implemented within a short period of time.

Amidst this significant change in the sanctions landscape, a major – and often overlooked - risk for financial institutions and the wider financial services sector are the expansive networks that may develop in order to facilitate the evasion of sanctions.

Below is a breakdown of a few recent examples of the networks and tactics that illicit organizations have orchestrated to evade sanctions as well as tactics that leading organizations can implement today to identify and combat sanctions evasion.

What are some examples of sanctions evasion networks and tactics?

Numerous examples have emerged in recent years, and have shown the extensive lengths that sanctioned states, individuals and businesses have gone to, in order to evade the restrictions imposed by international sanction regimes. These large and complex networks exhibit many of the same entities, tools, and structures typically seen with money laundering and terrorist financing typologies.

Some of these examples are set out below:

- On March 26th, 2019, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") took action against twenty-five individuals and entities. This included a network of Iranian, United Arab Emirates, and Turkey-based front companies. OFAC had identified that these entities had transferred over a billion dollars and euros to the Islamic Revolutionary Guard Corps ("IRGC") aand Iran's Ministry of Defence and Armed Forces Logistics ("MODAFL"), in addition to procuring millions of dollars worthdollars' worth of vehicles for MODAFL[6].
- The emergence of the use of advanced, emerging technology has also formed part of the sanctions evasion toolkit for sanctioned states. In September 2021, the United States Attorney for the Southern District of New York, announced that Virgil Griffith, a U.S. citizen, pleaded guilty to conspiring to violate the International Emergency Economic Powers Act ("IEEPA") by providing services to the Democratic People's Republic of Korea, including providing technical advice on using cryptocurrency and blockchain technology to evade sanctions.[7]
- From a Russian perspective, a press release from OFAC highlighted the role of such networks on March 31, 2022.[8] It highlighted how a Moscow-based engineering company was at the center of a procurement network engaged in proliferation

1 https://www.swift.com/news-events/news/message-swift-community
2 https://www.gov.uk/government/news/foreign-secretary-imposes-uks-most-punishing-sanctions-to-inflict-maximum-and-lasting-pain-on-russia
3 https://www.gov.uk/government/news/uk-hits-key-russian-oligarchs-with-sanctions-worth-up-to-10bn
4 https://ec.europa.eu/info/sites/default/files/business_economy_euro/banking_and_finance/documents/faqs-sanctions-russia-deposits_en.pdf
5 https://www.gov.uk/government/news/foreign-secretary-imposes-uks-most-punishing-sanctions-to-inflict-maximum-and-lasting-pain-on-russia
6 https://home.treasury.gov/news/press-releases/sm639
7 https://www.justice.gov/usao-sdny/pr/united-states-citizen-pleads-guilty-conspiring-assist-north-korea-evading-sanctions
8 https://home.treasury.gov/news/press-releases/jy0692

activities at the direction of the Russian Intelligence Services. This network operated across multiple countries to obfuscate the Russian military and intelligence agency end-users that relied on critical western technology. This network colluded to illicitly procure dual-use equipment and technology for Russia's defense sector. Similarly, on April 1, 2022, OFAC designated numerous entities and individuals involved in attempts to evade sanctions imposed by the United States and its international partners on Russia (which included a commercial bank and more than forty individuals and entities).[9]

- In a similar vein, the United States Financial Crimes Enforcement Network ("FinCEN") also highlighted the risk of Russian and Belarussian sanctions evasion networks in an alert issued to U.S. Financial Institutions on March 7, 2022[10]. This alert highlighted that Russian and Belarussian parties may attempt to evade sanctions through non-sanctioned Russian and Belarussian financial institutions in third countries, including through convertible virtual currency ("CVC") exchangers. It was specifically noted that "sanctioned persons, illicit actors, and their related networks or facilitators may attempt to use CVC and anonymizing tools to evade U.S. sanctions and protect their assets around the globe, including in the United States. CVC exchangers and administrators and other financial institutions may observe attempted or completed transactions tied to CVC wallets or other CVC activity associated with sanctioned Russian, Belarusian, and other affiliated persons". It was also interesting to note that FinCEN also encouraged financial institutions to also consider some of the tools and techniques associated with traditional money laundering schemes such as:

- The use of corporate vehicles to obscure (i) ownership, (ii) source of funds, or (iii) countries involved, particularly sanctioned jurisdictions.

- The use of shell companies to conduct international wire transfers.

- The use of third parties to shield the identity of sanctioned persons and/or PEPs seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.

How can organizations identify and combat sanctions evasion?

It is important for financial institutions and those in the wider financial sector to appreciate that the structures utilized to evade international sanctions regimes are increasingly complex and mirror many of the traits of traditional money laundering schemes.

It is crucial to understand that whilst screening of individual entities and customer lists against sanctions lists may help organizations identify whether a sanctioned entity or individual is either a client or attempting to become one, this will be insufficient in identifying any exposure to sanctions evasion networks. Assuming that an organisation has a mature sanctions compliance framework in place, which enables it to meet its regulatory obligations, there is an additional need for a more detailed investigative approach combining advanced forensic technology and business intelligence research.

Forensic technology and advanced data analytics, therefore, play an extremely important role in uncovering sanctions evasion networks and the extent to which they can infiltrate financial institutions. Network analytics provides the means through which the relationships between clients can be identified and fully understood.

This provides the means through which a holistic view of transactional activity and relationships can be gained, which can then be used to identify potential networks of illicit activity. This coupled with the use of detailed business intelligence investigation techniques provides a powerful combination to understand the extent of any sanctions evasion network exposure.

Conclusion

The invasion of Ukraine and the resulting economic sanctions provided an unprecedented scenario both for the wider world in terms of a changing geopolitical landscape, and also for the financial services sector in ensuring that those sanctioned cannot access global financial markets. However as has been highlighted previously, there is a long history of sanctioned entities, individuals, and states resorting to the use of sophisticated evasion networks, reminiscent of traditional money laundering and terrorist financing techniques.

While advances in new technology and cryptocurrencies can form an important part of such networks, the "traditional" tools of money launderers such as shell companies, wire transfers, property purchases, and corporate secrecy jurisdictions can all be used. It is therefore crucial that financial institutions and the wider financial services sector fully understand the extent to which such networks exist and can infiltrate their organiszations. Given the current geopolitical landscape, it may be increasingly likely that more sanctions will be imposed in the coming months. This could in turn lead to a greater proliferation of sanctions evasion networks and increased risk for the financial sector.

Henry Duggan
Senior Managing Director at Ankura

Andrew Pimlott
Senior Managing Director at Ankura

9 https://home.treasury.gov/news/press-releases/jy0731
10 https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf