Countering the Russian Federation's Use of Convertible Virtual Currency (CVC) for Sanctions Evasion

Summary

There is increasing concern about the use of convertible virtual currency (CVC) by Russian actors, including defense companies, to circumvent U.S. and other sanctions against the Russian Federation. Due to the increasing scale of sanctions from the U.S., European Union, United Kingdom, and other countries towards the Russian Federation, Russian actors may attempt to use CVCs to evade these measures. It is increasingly critical for all financial institutions to understand the use of CVC to evade sanctions, identify red flags, and establish comprehensive due diligence practices as well as information sharing best practices.

Background on Convertible Virtual Currencies

Convertible virtual currency is an unregulated digital currency that can be used as a substitute for real and legally recognized currency even though it does not have the status of legal tender. The decentralized and underregulated nature of crypto can be used as a vehicle for illicit transactions, including as a means for Russian individuals and entities to bypass sanctions, protect their assets, and be able to participate in the global financial system. However, all anti-money laundering countering the financing of terrorism/counter-proliferation (AML/CFT/CP) and sanctions compliance obligations apply to CVC transactions.

Russian Federation's Use of Convertible Virtual Currencies: Trends

There are several trends to be aware of regarding the Russian Federation's use of CVCs to evade sanctions:

- It is likely that private sector actors, such as sanctioned individuals and entities, will attempt to use CVCs;
- Russia will loosen regulations on CVCs to facilitate cryptocurrency transfers by private state actors or sanctioned persons;

- Russian state actors may use CVCs to fund intelligence operations and cyberattacks, including the use of ransomware attacks and hacks targeting CVC exchanges.

Red Flags for the Private Sector

All financial institutions and money services businesses, including CVC exchangers and administrators, must be aware of red flags associated with sanctions evasion using CVC. Several of these red flags include:

- The use of CVCs and CVC-anonymizing tools by sanctioned persons and their networks for facilitators to evade sanctions and protect their assets internationally;
- A customer's transactions are initiated from or sent to the following types of Internet Protocol (IP) addresses: non-trusted sources; locations in Russia, Belarus, FATF-identified jurisdictions with AML/CFT/CP deficiencies, and comprehensively sanctioned jurisdictions; or IP addresses previously flagged as suspicious;
- A customer's transactions are connected to CVC addresses listed on the United States' Office for Foreign Asset Control's Specially Designated Nationals and Blocked Persons List;
- A customer uses a CVC exchanger or foreign-located MSB in a high-risk jurisdiction with AML/CFT/CP deficiencies, particularly for CVC entities and activities, including inadequate "know-your-customer" or customer due diligence measures.

Implications for FI Compliance and Due Diligence

Given the risks associated with transactions potentially linked to Russian actors using CVC to evade sanctions, FIs and Virtual Asset Service Providers should review their sanctions compliance programs to ensure that risks associated with illicit CVC activity, including the use of CVCs to evade sanctions, are fully integrated into their policies, procedures, and controls. They must also ensure that they have the tools and resources to comprehend sanctions and other illicit finance risks

associated with counterpart wallet addresses. Several concrete steps that can be taken to ensure compliance include:

- Enhanced screening and scrutiny of relationships with Virtual Asser Service Providers in jurisdictions with weak or undeveloped AML/CFT regimes;
- Conducting periodic risk assessments to assess sanctions exposure risks and identify steps to minimize those risks;
- Consider implementing CVC transaction monitoring tools.