SheppardMullin

Global Trade Law Blog

Timely Updates and Analysis on Key International Trade Law Issues

Crypto and Russia Sanctions: A Primer and Survival Guide For Crypto Companies

By Pouneh Almasi, Sarah Aberg, Reid Whitten & Fatema Merchant on March 17, 2022

POSTED IN SANCTIONS

The recent comprehensive economic sanctions by the U.S. and other nations against Russia has propelled the crypto community onto the geo-political stage in a major way. As visibility—in reassurance of it. As discussed below, there are several steps that crypto platforms can take to further efforts in blocking and detecting sanctions evasion activity on their platforms.

I. Cryptocurrency-Related Uses in Sanction Evasion

There are multiple ways that cryptocurrency technology can be harnessed to evade the sanctions on Russia. This is particularly important given this volume of illicit assets that originate or are transmitted through Russia. According to blockchain-tracking analysts, about 74 percent of the global ransomware revenue last year went to entities likely affiliated with Russia.**[1]**

- **Digital Ruble**—The Russian government is developing a digital ruble, its own Central Bank Digital Currency, that it could use to trade directly with other countries that accept the digital currency without first converting it into U.S. dollars. This would undermine and lessen the intended economic pressures of U.S. sanctions on Russia.
- **Anonymity-Enhanced Cryptocurrencies (AECs)**—AECs are a relatively new type of cryptocurrency that further reduce the transparency of crypto transactions and financial flows. AECs could be utilized by sanctioned entities to hide their identities and avoid blocks on exchange platforms.
- **Mixing Services**—Mixers enable users to conceal or further obfuscate the source or owner of cryptocurrency to prevent others from tracing a transmission back to its source. Like AECs, the use of mixing services would enable sanctioned entities to conceal their identities and escape detection.
- **Multiple Wallet Addresses**—Wallets are easy to open, and sanctioned actors can open up multiple wallets to move funds from a flagged or blacklisted wallet to a new

- **Foreign Centralized Exchanges**—Centralized exchanges in high-risk jurisdictions with inadequate anti-money laundering (AML) compliance standards have been linked to transfers of illicit funds, particularly as preferred cash-out points in the process of laundering funds in cryptocurrency to fiat currency.
- **Chain Hopping**—Chain hopping refers to the process of converting one cryptocurrency into a different cryptocurrency at least once before moving the funds to another platform (e.g., a customer account that receives cryptocurrency from an external wallet and subsequently initiates multiple trades among multiple cryptocurrencies, often in rapid succession). Sanctioned actors can use this practice to make it harder to trace their transaction history back to the original blockchain, and has been linked to transfers of illicit funds.

II. Risk Mitigation Strategies

There are several risk mitigation measures that crypto platforms, such as exchanges and wallets, can utilize to block and detect attempts to engage in sanctioned activity on their platforms:

***Blocking access by sanctioned entities**:*

- Screen account applications against lists of sanctioned entities
- Require identifying information, such as names and countries of residence, and validate this information against Internet Protocol (IP) addresses and publicly available information
- Utilize geofencing controls to block IP addresses from sanctioned countries

***Detecting evasion attempts**:*

  indicators, including:
    - Customer transactions initiated from or sent to IP addresses from non-trusted sources; locations in Russia, Belarus, **FATF**-identified high-risk jurisdictions with AML deficiencies, and **comprehensively sanctioned jurisdictions**
    - Customer transactions connected to wallet addresses listed on **OFAC**'s Specially Designated Nations and Blocked Persons List
    - Use of foreign-located exchanges in **FATF**-identified high-risk jurisdictions with AML deficiencies, including inadequate "know-your-customer" or customer due diligence measures
- Develop transaction monitoring protocols to detect "red flag" indicators of activity associated with ransomware payments, such as:
    - Customer accounts that receive cryptocurrency from an external wallet and subsequently initiates multiple, rapid trades among multiple cryptocurrencies with no apparent related purpose, followed by a transaction off the platform
    - Initiating transfers of funds involving a cryptocurrency mixing service

Anticipate potential threats:

- Utilize blockchain analytics programs to detect high-risk behavior
- Stay up-to-date on trends identified in regulatory guidance

Crypto platforms should make sure to have compliance programs in place to avoid fines by regulators, and consult with experienced attorneys for additional guidance and expertise.

Global Trade Law Blog