Articles + Publications | March 16, 2022

FinCEN Implores Vigilance From Financial Institutions in Anticipation of Attempted Russia Sanctions Evasion

WRITTEN BY

Keith J. Barnett | Ethan G. Ostroff | Kalama M. Lui-Kwan | Ghillaine A. Reid | Carlin A. McCrory | Jay A. Dubow | Angela Monaco

Following the significant sanctions and other restrictions imposed by the United States and its global allies resulting from the Russian Federation's invasion of Ukraine, the Financial Crimes Enforcement Network (FinCEN) issued an alert (FinCEN Alert) on March 7, advising financial institutions on how to identify and report potential attempts to evade sanctions.

The FinCEN Alert provides a number of red flags associated with potential sanctions evasion using the U.S. financial system and convertible virtual currency (CVC). These include:

- Use of corporate vehicles to obscure (1) ownership, (2) source of funds, or (3) countries involved, particularly sanctioned jurisdictions;
- Use of shell companies to conduct international wire transfers, often involving financial institutions in jurisdictions distinct from company registration;
- Use of third parties to shield the identity of sanctioned persons and/or politically exposed persons (PEPs) seeking to hide the origin or ownership of funds, such as hiding the purchase or sale of real estate;
- Accounts in jurisdictions or with financial institutions experiencing a sudden rise in value being transferred to their respective areas or institutions, without a clear economic or business rationale;
- Jurisdictions previously associated with Russian financial flows identified as having a notable increase in new company formations;
- Newly established accounts that attempt to send or receive funds from a sanctioned institution or an institution removed from the Society for Worldwide Interbank Financial Telecommunication;
- Nonroutine foreign exchange transactions that may indirectly involve sanctioned Russian financial institutions, including transactions inconsistent with activity over the prior 12 months;
- Customer's transactions initiated from or sent to the following types of Internet Protocol (IP) addresses: nontrusted sources; locations in Russia, Belarus, Financial Action Task Force-identified jurisdictions with anti-money laundering/countering the financing of terrorism/counter proliferation (AML/CFT/CP) deficiencies, and comprehensively sanctioned jurisdictions; or IP addresses previously flagged as suspicious;

- Customer's transactions connected to CVC addresses listed on any of the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) Lists; and

- Customer's use of a CVC exchanger or foreign-located money services business 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.

FinCEN also warned of the dangers posed by Russian-related ransomware campaigns, offering additional red flag indicators of Russian and other ransomware and cybercrime activities:

- A customer receives CVC from an external wallet, and immediately initiates multiple, rapid trades among multiple CVCs with no apparent related purpose, followed by a transaction off the platform, which may be indicative of attempts to break the chain of custody on the respective blockchains or further obfuscate the transaction;

- A customer initiates a transfer of funds involving a CVC mixing service; and

- A customer has either direct or indirect receiving transaction exposure identified by blockchain tracing software as related to ransomware.

If a financial institution detects suspicious activity as defined in the FinCEN Alert, FinCEN requests that it file a Suspicious Activity Report (SAR) by using the key term "FIN-2022-RUSSIASANCTIONS" in SAR Field 2 (Filing Institution Note to FinCEN) and the narrative.

In addition to urging financial institutions to identify and promptly report suspicious activity potentially indicative of sanctions evasion, FinCEN emphasized that all financial institutions should conduct appropriate risk-based customer due diligence and take advantage of their ability to share information under Section 314(b) of the USA PATRIOT Act to help identify hidden Russian and Belarusian assets.

Financial institutions should promptly and carefully review and update their AML, Bank Secrecy Act (BSA), OFAC, and other related procedures to meet the obligations imposed by the FinCEN Alert, including any necessary training on the red flag indicators and the new SAR filing instructions associated with sanctions evasion activity. Financial institutions also should continue to monitor the sanctions list and related OFAC guidance updates to ensure adherence to the evolving requirements and prohibitions.

RELATED INDUSTRIES + PRACTICES

- Consumer Financial Services
- Securities Investigations + Enforcement
- White Collar Litigation + Investigations