KPMG

Regulatory Alert

Regulatory Insights

March 2022

U.S. actions to Russia-Ukraine war: FinCEN Alert

Financial services companies are facing rapid and iterative regulatory expectations around current and expected OFAC sanctions and Administration executive orders. Regulators will expect companies to apply tight controls around areas of currently heightened risk given the Russian government's ongoing attack on Ukraine, including sanctions compliance, financial crimes, cyber security, and crypto and digital assets. FinCEN's Alert focuses attention to key BSA/AML/CTF areas such as beneficial ownership, crypto and digital asset transactions, ransomware attacks and payments, and customer due diligence.

The Department of the Treasury, Financial Crimes Enforcement Network (FinCEN) issued an Alert advising all financial institutions to be vigilant against attempts to circumvent sanctions and other restrictions recently imposed on Russian and Belarusian financial institutions and other designated entities and individuals. (*See KPMG Regulatory Alerts, here and here.*) The Alert outlined select "red flags" to assist in identifying potential sanctions evasion activity through a number of different channels, including the U.S. financial system, convertible virtual currency (CVC) transactions, and cybercrime. In addition, the Alert outlines Bank Secrecy Act (BSA) reporting obligations, including with respect to CVC, and links to multiple FinCEN publications on related topics and guidance.

Potential sanctions evasion activity through multiple channels

— ***The U.S. financial system.*** FinCEN suggests sanctioned Russian and Belarusian actors may seek to evade sanctions through a variety of means, including:

- Use of corporate vehicles (i.e., legal entities, such as shell companies, and legal arrangements) to obscure i) ownership, ii) source of funds, or iii) 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 PEPs (politically exposed persons) seeking to hide the origin or ownership of funds, for example, to hide the purchase or sale of real estate.
- Accounts in jurisdictions or with financial institutions that are 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 that are identified as having a notable recent increase in new company formations.
- Newly established accounts that attempt to send or receive funds from a sanctioned institution or an institution removed from SWIFT (Society for

Worldwide Interbank Financial Telecommunication).

- Foreign exchange transactions that may indirectly involve sanctioned Russian financial institutions, including transactions that are inconsistent with activity over the prior 12 months.

— ***CVC transactions.*** CVC exchangers and administrators are generally considered money services businesses (MSBs) under the BSA. FinCEN cautions that CVC exchangers and administrators and other financial institutions may observe attempted or completed transactions tied to CVC wallets or other CVC activity that are associated with sanctioned Russian, Belarusian, and other affiliated persons. Activities that may raise "red flags" include:

- 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 (anti-money laundering/countering the financing of terrorism/counter proliferation) deficiencies, and comprehensively sanctioned jurisdictions; or to or from IP addresses previously flagged as suspicious.
- A customer's transactions are connected to CVC addresses listed on OFAC'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 customer due diligence measures.

— ***Ransomware and other cybercrime.*** Select "red flag" indicators of ransomware and other cybercrime activity include instances where 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.
- Initiates a transfer of funds involving a CVC mixing service.
- Has either direct or indirect receiving transaction exposure identified by blockchain tracing software as related to ransomware.

BSA obligations and tools

— ***Suspicious Activity Reports.*** Financial institutions (including MSBs) are required to file a SAR (Suspicious Activity Report) if they know, suspect, or have reason to suspect a transaction conducted or attempted by, at, or through the financial institution involves funds derived from illegal activity, or attempts to disguise funds derived from illegal activity; is designed to evade regulations promulgated under the BSA; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including sanctions evasion.

- Additional reports are required to be filed with OFAC in certain instances involving designated persons and ransomware attacks and payments.

— ***Due diligence***. The Alert outlines and reiterates due diligence obligations related to i) senior foreign political figures, ii) private banking accounts, and iii) correspondent accounts.

— ***Information sharing***. FinCEN strongly encourages, at the critical time, voluntary information sharing under the safe harbor authorized by section 314(b) of the USA PATRIOT Act. It reminds financial institutions that they may share information with one another regarding individuals, entities, organizations, and countries suspected of possible terrorist financing or money laundering.

Financial Action Task Force

Separately, the Financial Action Task Force (FATF) announced final updates to its Recommendation 24, which are intended to improve transparency of **beneficial ownership** of legal persons. The updates require countries to take a multi-pronged approach for collection of beneficial ownership information including:

— Requiring companies to obtain and hold adequate, accurate and up-to-date information on their own beneficial ownership and make such information available to competent authorities in a timely manner.

— Requiring beneficial ownership information to be held by a public authority or body functioning as beneficial ownership registry or use of an efficient alternative mechanism

— Applying any additional supplementary measures necessary to ensure the determination of beneficial ownership of a company, including holding beneficial ownership information obtained by regulated financial institutions and professionals, or held by regulators or in stock exchanges.

FATF also announced the release of draft guidance on the risk-based implementation of AML/CTF measures in the **real estate sector**.

FinCEN has previously released proposals of their own on both beneficial ownership and real estate transactions. (*See KPMG Regulatory Alert, here.*)

Note: The FATF is an intergovernmental, international standards setting body comprised of more than 200 countries and jurisdictions focused on anti-money laundering and countering terrorist financing activities.

For additional information, please contact Amy Matsuo, Tom Keegan, or John Caruso.

Watch for it! KPMG Regulatory Insights will publish shortly a Point-of-View on current regulatory developments in the U.S. crypto and digital assets markets.

Contact the author:

Amy Matsuo
Principal and Leader
Regulatory and ESG Insights
amatsuo@kpmg.com

kpmg.com/socialmedia

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.