

FinCEN Urges Financial Institutions to Guard Against Attempts to Evade Sanctions

by Erin Bryan, Joseph Lynyak, and Lawrence Ward

On March 7, 2022, the Financial Crimes Enforcement Network (“FinCEN”) issued an alert (the “FinCEN Alert”) urging financial institutions to proactively guard against possible attempts to evade recently implemented sanctions and other restrictions in connection with the Russian Federation’s invasion of Ukraine.¹ This Dorsey eUpdate discusses the FinCEN Alert and outlines steps financial institutions can take to ensure compliance.

Recent Ukraine-Related Treasury Actions

The FinCEN Alert follows numerous recent actions by the U.S. Government in response to Russian aggression against Ukraine and in furtherance of Executive Order 14024, issued April 15, 2021 (“EO 14024”)², and Executive Order 14065 (“EO 14065”), issued February 21, 2022, which announced new sanctions and other restrictions on Russia and the occupied territories of Ukraine.

On February 22, 2022, Office of Foreign Assets Control (“OFAC”) of the U.S. Department of the Treasury (the “Treasury”) issued its *Determination Pursuant to Section I(a)(i) of Executive Order 14024*, which provides that section I(a)(i) of EO 14024 shall apply to the financial services sector of the Russian Federation economy.³ In the following days and weeks, OFAC issued a further series of notices adding individuals, entities, and vessels to its Specially Designated Nationals and Blocked Persons List (“SDN List”), List of Foreign Financial Institutions Subject to Correspondent Account or Payable-Through Account Sanctions (“CAPTA List”), and Non-SDN Menu-Based Sanctions List (“NS-MBS List”) (collectively, the “OFAC Lists”).⁴

On March 8, 2022, the White House issued its Executive Order 14066 (“EO 14066”) to prohibit any U.S. person from engaging in (i) the importation from Russia of crude oil, petroleum or distilled petroleum products, liquefied natural gas or coal or coal products; (ii) investments and financings in connection with, or relating to, the energy sector of the Russian Federation’s economy; or (iii) the approval, financing, facilitation or guarantee of

Related People

- Erin Bryan
- Joseph Lynyak
- Lawrence Ward

Related Capabilities

- Banking & Financial Institutions
- Financial Services Regulatory
- National Security Law
- International Trade

any such transaction by a foreign person if a U.S. person would be prohibited from engaging in such transaction.⁵

In recent weeks, the Treasury Department has issued a number of press releases and FAQs, which further clarify Treasury's expectations concerning the implementation of these recent Russian Federation-related sanctions and restrictions (collectively, the "Russia Sanctions").⁶

The FinCEN Alert

The FinCEN Alert highlights the critical role of financial institutions in preventing attempts to evade the Russia Sanctions, identifies numerous "Red Flags" that could indicate attempts to evade the Russia Sanctions, reminds financial institutions about the risks of Russian-related ransomware and other cybercrime attacks, provides new filing instructions for suspicious activity reports ("SARs") relating to the Russia Sanctions, and emphasizes the obligations of financial institutions to conduct adequate customer due diligence and report suspicious activities, including in regard to convertible virtual currency.

a. Red Flags

The FinCEN Alert includes lists of Red Flags indicative of possible attempts to evade the Russia Sanctions, including the following:

- Use of corporate vehicles (*i.e.*, legal entities such as shell companies or legal arrangements) to obscure: (i) ownership; (ii) source of funds; or (iii) countries involved, particularly sanctioned jurisdictions' ransomware and cybercrime attacks;
- 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 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 the Society for Worldwide Interbank Financial Telecommunication ("SWIFT");
- Non-routine foreign exchange transactions that may indirectly involve sanctioned Russian financial institutions, including transactions that are inconsistent with activity over the prior 12 months;
- 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, 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;

- A customer's transactions are connected to convertible virtual currency addresses listed on any of the OFAC Lists; or
- A customer uses 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 intends the foregoing non-exhaustive list to supplement existing FinCEN guidance on Red Flags.

b. Reporting Suspicious Activity

Under existing AML/CFT/CP laws and regulations, covered financial institutions must file a SAR "if it knows, suspects, or has 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."⁷ Filing SARs for other suspicious activity is permitted. If a financial institution detects suspicious activity within the scope of the FinCEN Alert, FinCEN requests that it file a SAR and reference the FinCEN by including the key term "FIN-2022-RUSSIASANCTIONS" in SAR field 2 (Filing Institution Note to FinCEN), and by noting in the narrative the connection between the suspicious activity being reported and the activities highlighted in the FinCEN Alert. Financial institutions may expedite reports of such Russia Sanctions-related suspicious activities highlighted in the FinCEN Alert by also calling the FinCEN Financial Institutions Toll-Free Hotline at (866) 556-3974. Suspicious activity involving ransomware or cyber attacks that appears to have a nexus to the Russia Sanctions must be immediately reported to FinCEN, and accompanied by a SAR filing FinCEN's BSA E-filing System. The FinCEN alert emphasizes that these reporting requirements are in addition to financial institutions' existing obligations related to Currency Transaction Reports, Report of Cash Payments Over \$10,000 Received in a Trade or Business (Form 8300), Report of Foreign Bank and Financial Accounts, Report of International Transportation of Currency or Monetary Instruments, Registration of Money Service Business, and Designation of Exempt Person.

Risk Management for Financial Institutions

In light of the global threat presented by the Russian incursion into Ukraine, compliance with the FinCEN Alert should be considered the highest priority by banks and other financial institutions. In the minimum, a financial institution should adequately document that its AML and OFAC processes have been updated, and staff responsible for identifying and reporting Red Flags are thoroughly trained and constantly updated as the scope of the Russia Sanctions evolves.

Financial institutions should be aware that OFAC has also issued express general licenses with "wind-down" periods that will explicitly allow their customers to complete certain in-process sales or purchases or other similar transactions before specified

dates. Many responsible customers will likely reach out to communicate with their own financial institutions to discuss proposed payments or other transactions that could potentially implicate the Russia Sanctions and to disclose their intention to rely upon OFAC general licenses or other such authorizations. Candid and timely communications with financial institutions can thus avoid misunderstandings and mistakes that could otherwise strain institution-customer relations and disrupt or delay lawful transactions that the Russia Sanctions are not actually intended to prevent. However, because there is no harm in filing a SAR, in light of the potential legal risk for failing to report potential Red Flags, financial institutions may want to err on the side of caution and file SARs in situations in which collaborative evidence is unclear or uncertain.

In addition to this compliance approach, financial institutions should undertake the following steps:

- Immediately and continually review the most current OFAC Lists to ensure that the financial institutions are not allowing prohibited persons to move assets through the U.S. financial system;
- Update their AML and Bank Secrecy Act procedures to reflect the new SAR filing instructions, including by directing personnel to include the “FIN-2022-RUSSIASANCTIONS” key term where applicable;
- Ensure that ransomware attacks are reported immediately;
- Update their AML and Bank Secrecy Act procedures to include additional red flag indicators where appropriate; and
- Train personnel on the new obligations imposed by FinCEN in connection with the Russia Sanctions.

Finally, financial institutions must continue to actively monitor the quickly-evolving developments from the White House and Treasury to ensure that compliance programs remain consistent with regulators’ expectations. Financial institutions should also be mindful that their own customers are also trying to understand and comply with the new Russia Sanctions at the same time and to adjust their own business practices in good faith as quickly as possible to meet such new requirements and prohibitions.

* * *

We trust this summary and analysis of the FinCEN Alert is useful, and may assist in banks and other financial institutions implementing appropriate compliance processes. In light of what may be rapidly evolving obligations to the Russian Sanctions, Dorsey attorneys are available to assist in obtaining clarifications from FinCEN and OFAC for our clients. If you have any questions regarding this eUpdate, please contact the attorneys profiled below.

¹ FinCEN FIN-2022-Alert001 of March 7, 2022, *FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts*, available at: <https://www.fincen.gov/sites/default/files/2022-03/FinCEN%20Alert%20Russian%20Sanctions%20Evasion%20FINAL%20508.pdf> (last accessed March 9, 2022).

² See Executive Order 14024 of April 15, 2021, *Blocking Property With Respect To*

Specified Harmful Foreign Activities of the Government of the Russian Federation, available at: <https://home.treasury.gov/system/files/126/14024.pdf> (last accessed March 9, 2022); Executive Order 14065 of February 21, 2022, *Blocking Property of Certain Persons and Prohibiting Certain Transactions With Respect to Continued Russian Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine*, available at: <https://www.whitehouse.gov/briefing-room/presidential-actions/2022/02/21/executive-order-on-blocking-property-of-certain-persons-and-prohibiting-certain-transactions-with-respect-to-continued-russian-efforts-to-undermine-the-sovereignty-and-territorial-integrity-of-ukraine/> (last accessed March 9, 2022).

³ OFAC *Determination Pursuant to Section I(a)(i) of Executive Order 14024* (February 22, 2022), available at:

https://home.treasury.gov/system/files/126/russia_harmful_determination_20220222.pdf (last accessed March 9, 2022). Section I(a)(i) of EO 14024 allows the Secretary of the U.S. Department of the Treasury to block transactions with persons the Secretary has determined “to operate or have operated in the technology sector or the defense and related materiel sector of the Russian Federation economy, or any other sector of the Russian Federation economy as may be determined by the Secretary of the Treasury, in consultation with the Secretary of State.”

⁴ A complete list of OFAC’s recent actions is available at:

<https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions> (last accessed March 9, 2022).

⁵ See Executive Order of March 8, 2022, *Prohibiting Certain Imports and New Investments With Respect to Continued Russian Federation Efforts to Undermine the Sovereignty and Territorial Integrity of Ukraine*, available at:

https://home.treasury.gov/system/files/126/eo_prohibitions_imports_investments.pdf (last accessed March 9, 2022).

⁶ A complete list of OFAC’s recent new and amended “Frequently Asked Questions” is available at: <https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions> (last accessed March 9, 2022).

⁷ FinCEN Alert at p. 5 (citing 31 CFR § 1020.320, 1021.320, 1022.320, 1023.320, 1024.320, 1025.320, 1026.320, 1029.320, and 1030.320).