Wolters Kluwer

Russian sanctions: Compliance, enforcement, and the prevention of sanctions evasion

SPECIAL REPORT | The Ukraine Crisis

By Katalina M. Bianco, J.D.

Since February 2022, there has been a flurry of U.S.-imposed sanctions on Russia stemming from its invasion of Ukraine. In keeping with President Joseph Biden's February 21 executive order and with its initial sanctions of February 22, the United States took "significant and unprecedented action" to respond to Russia's further invasion of Ukraine, targeting Russia's largest banks, state-run companies, the bulk of its financial institution subsidiaries, and Russian elites and their families. With the speed at which sanctions are being imposed, financial institutions and the law firms and attorneys counseling them are scrambling to navigate the rules and regulations intended to ensure compliance with the sanctions and trade embargoes against Russia and prevent potential Russian sanction evasion attempts.

A statement on the Ukraine situation by the Financial Action Task Force (FATF), published earlier this March, puts into perspective the serious risks associated with sanctions evasion. The FATF expressed "its grave concern about the invasion's impact on the money laundering, terrorist financing and proliferation financing (MLTF/PF) risk environment as well as the integrity of the financial system, the broader economy and safety and security." The FATF called on jurisdictions to provide advice and facilitate information sharing with their private sectors on assessing and mitigating any emerging MLTF/PF risks identified, including in relation to virtual assets, as well as other threats to international safety and security from the region. The FATF noted that all jurisdictions should be vigilant to the possibility of emerging risks from circumvention of measures taken in order to protect the international financial system from the ML/TF/PF risks resulting from Russia's aggression against Ukraine.

Vigilance to the possibility of sanction evasion and the associated risk to the international financial system requires heightened monitoring of activity by the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) and compliance with its regulations. That may mean freezing assets or interests in properties owned by entities and individuals on OFAC's Specially Designated Nationals (SDN) List or cutting ties to Russian and Belarusian clients. Closely understanding and adhering to OFAC guidance on sanction compliance can provide institutions and their counselors with the tools for successful compliance. Added to the OFAC compliance is guidance provided to financial institutions by the Financial Crimes Enforcement Network (FinCEN) on preventing potential Russian sanctions evasions. FinCEN's "red flags" can act as a checklist for institutions seeking to identify suspicious activity associated with potential sanctions evasion.

OFAC guidance. OFAC strongly recommends in its compliance framework that organizations under U.S. jurisdiction and foreign entities that conduct business in or with the United States, U.S. persons, or using U.S.-origin goods or services, develop a risk-based approach to sanctions compliance. The means to this approach is to implement and monitor a sanctions compliance program (SCP) tailored to a company's size, products and services, and customers. The SCP should consist of five elements:

Management commitment to the program – Effective management support includes the provision of adequate resources to the compliance unit(s) and support for compliance personnel's authority within an organization. The organization should have a dedicated OFAC sanctions compliance officer reporting to management.

Risk assessment – Risks in sanctions compliance are potential threats or vulnerabilities that may lead to violations of OFAC's regulations and negatively affect an organization's reputation and business. Conducting a routine risk assessment of specific clients, products, services, and geographic locations is an integral means to identify and handle potential OFAC issues and mitigate risks.

Internal controls – The purpose of internal controls is to outline clear expectations, define procedures and processes pertaining to OFAC compliance, including reporting and escalation chains, and minimize the risks

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

identified by the organization's risk assessments. Policies and procedures should be enforced, weaknesses should be identified and remediated, and internal and external audits and assessments of the program should be conducted on a periodic basis. An effective SCP should be capable of adjusting rapidly to changes published by OFAC, such as updates to OFAC's List of Specially Designated Nationals and Blocked Persons or new guidance.

Testing/auditing – A comprehensive and objective testing or audit function within an SCP ensures that an organization identifies program weaknesses and deficiencies. It is the organization's responsibility to enhance its program and to remediate any identified compliance gaps. The organization must commit to ensuring that the testing or audit function is accountable to senior management, independent of the audited activities and functions, and has sufficient authority, skills, expertise, resources, and authority within the organization.

Training – An effective SCP includes a strong training program. The training program should be provided to all appropriate employees and personnel on a periodic basis (at least annually) and generally should provide job-specific knowledge based on need, communicate the sanctions compliance responsibilities for each employee, and hold employees accountable for sanctions compliance training through assessments.

A strong and effective SCP may mitigate any civil money penalties levied by OFAC in response to an apparent violation. OFAC also may, in appropriate cases, consider the existence of an effective SCP at the time of an apparent violation as a factor in its analysis as to whether a case is deemed "egregious." OFAC recommends that all organizations subject to U.S. jurisdiction review the settlements published by OFAC to reassess and improve their respective SCPs.

OFAC SCP deficiencies. OFAC recommends scrutinizing prior OFAC enforcement actions in which the agency identified SCP deficiencies and their root causes to get a sense of how OFAC imposes civil money penalties (CMPs)and insight into related mitigating and aggravating factors.

Some of the root causes of deficient SCPs identified by OFAC include:

- Lack of a formal SCP;
- Misinterpreting or misunderstanding OFAC regulations (for example, organizations failing to consider that OFAC sanctions applied to their organization based on their status as a U.S. person, a U.S.-owned or controlled subsidiary, or dealings in or with U.S. persons, the U.S. financial system, or U.S.-origin goods and technology);
- Aggravating factors such as reckless conduct, the presence of numerous warning signs that the activity at issue was likely prohibited, or awareness by the organization's management of the conduct at issue; engaging in transactions or activity that violated OFAC's regulations by referring business opportunities to, approving or signing off on transactions conducted by, or otherwise facilitating dealings between their organization's non-U.S. locations and OFAC-sanctioned countries, regions, or persons;
- Non-U.S. persons purchasing U.S.-origin goods with the specific intent of reexporting, transferring, or selling the items to a person, country, or region subject to OFAC sanctions;
- Non-U.S. persons processing financial transactions to or through U.S. financial institutions that relate to commercial activity involving an OFAC-sanctioned country, region, or person;
- Failing to update sanctions screening software;
- Failing to conduct proper due diligence on customers, clients, supply chains, intermediaries, and counter-parties; and
- Using non-standard payment or commercial practices.

OFAC also notes that individual employees have in some instances played roles in causing, or at least facilitating, OFAC regulatory violations. OFAC has identified situations involving U.S.- owned or controlled entities operating outside of the United States, in which supervisory, managerial or executive employees of the entities conducted or facilitated dealings or transactions with OFAC-sanctioned persons, regions, or countries, despite the fact that the U.S. entity had an extensive SCP in place.

FinCEN flags. FinCEN's March alert advises financial institutions to be on the watch for efforts to evade sanctions in connection with the Russian invasion of Ukraine. The alert provides red flags intended to assist institutions in identifying suspected evasion activity and stresses Bank Secrecy Act reporting obligations. FinCEN believes that the economic pressures on Russia and Belarus stemming from the sanctions may result in "sanctions evasion that may occur through various means, including through currently unsanctioned Russian and Belarusian banks or other financial institutions that retain at least some access to the international financial system." FinCEN noted that although large scale sanctions evasion using convertible virtual currency (CVC) by the Russian government might not be feasible, CVC exchangers and administrators, as well as other financial institutions, may see

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.

transactions connected to CVC wallets or other CVC activity that are associated with sanctioned Russian, Belarusian, and other affiliated individuals. Anti-money laundering/countering the financing of terrorism/ counter proliferation (AML/CFT/ CP) and sanctions compliance obligations apply to CVC transactions, just as they do to transactions involving fiat currency.

The alert also reminds financial institutions of the dangers posed by Russian-related ransomware campaigns. FinCEN encourages financial institutions to review FinCEN's previous publications to review indicators relevant to foreign political corruption and efforts by corrupt senior foreign political figures, their families, and their associates (often referred to as foreign "politically exposed persons" or PEPs), or associated entities and financial facilitators, to evade U.S. sanctions or otherwise hide their assets.

Specific red flag indicators include:

- Use of corporate vehicles such as shell companies to obscure ownership, source of funds, or 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 seeking to hide the origin or ownership of funds.
- 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.
- 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 connected to CVC addresses listed on OFAC's Specially Designated Nationals and Blocked Persons List.

FinCEN also reminds institutions that a financial institution is required to file a Suspicious Activity Report 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 Bank Secrecy Act; lacks a business or apparent lawful purpose; or involves the use of the financial institution to facilitate criminal activity, including sanctions evasion.

Information sharing. OFAC, FinCEN, and the FATF emphasized the importance of information sharing among government entities. Financial institutions and their management should take note of state actions taken to strengthen the enforcement of sanctions. For example, Kathy Hochul, Governor of New York, announced steps intended to strengthen the New York Department of Financial Services' (DFS) enforcement of sanctions against Russia. The DFS will expedite the procurement of additional blockchain analytics technology in order to detect exposure among DFS-licensed virtual currency businesses to Russian individuals, banks, and other entities that have been sanctioned. Leveraging purpose-built technologies and service providers for virtual currency protects the financial system from illicit activity including money laundering, terrorist financing and ransomware activity. This action followed an executive order by Hochul directing all New York State agencies and authorities to review and divest public funds from Russia following Russia's attack on Ukraine.

Conclusion. Sanctions compliance and the prevention of actions taken as a back-door means to evade sanctions requires diligence, strict monitoring of OFAC's SDN List, and the implementation of OFAC and FinCEN guidance, starting with an effective SCP that is wholly supported by management. ■

©2022 CCH Incorporated and its affiliates. All rights reserved. Reprinted with permission from CCH Incorporated.