KPMG

Regulatory Alert

Regulatory Insights

March 2022

U.S. actions to Russia-Ukraine war: New Sanctions, Evasion Coordination & Cyber Risks

The U.S. Treasury has imposed expanded sanctions, and the Administration has heightened alerts for potential sanctions evasion as well as cyber risks. Companies should not only comply with these evolving sanctions, but also look to assess, enhance, and invest in their sanctions compliance program considering OFAC's 2019 framework across five essential components: management commitment, risk assessment, internal controls, testing and auditing, and training. (See KPMG Regulatory Alert, here.) The Administration has also urged companies to implement several cybersecurity measures in anticipation of potential Russian cyber-attacks in response to the sanctions. Companies should consider how the Russia-Ukraine war could develop, scenarios that could arise, and the implications of each scenario on the company's people, businesses, supply chains, and technology, with cybersecurity as one element of this broader view.

Additional Sanctions

The Department of the Treasury's Office of Foreign Assets Control (OFAC) announced additional sanctions to be imposed on numerous Russian companies and individuals designated as "key enablers" of the Russia-Ukraine war. Actions include:

- Designation of multiple companies that are active parts of Russia's defense-industrial base
- Designation of the Chairman and CEO of Russia's largest financial institution, Sberbank (Public Joint Stock Company Sberbank of Russia)
- Designation of 328 members (out of 450) of Russia's state legislative body, the Duma
- Issuance of new guidance (FAQs) reiterating that transacting in gold with the Russian Central Bank is prohibited under existing sanctions

As a result of OFAC's actions, all property and interests in property of the covered individuals and companies that are in the U.S. or U.S. possession are blocked and must be reported to OFAC, including any entities that are owned, directly or indirectly, 50 percent or more by one or more blocked persons are also blocked.

All transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons are prohibited unless authorized by a license issued by OFAC or another exemption.

Sanctions Evasion

Russian Central Bank. In coordination with G7 and EU nations, the Administration announced a sanctions evasion initiative to share information about and coordinate responses related to circumvention and backfilling of existing sanctions, including blunting the Russian Central Bank's ability to deploy international reserves and gold.

Cryptocurrencies. Notably, earlier this month, Federal Reserve Board Chair Powell addressed concerns about

whether cryptocurrencies could be used to bypass sanctions, stating that the concerns "underscore the need for congressional action on digital finance including cryptocurrencies" to establish the kind of regulatory framework that is "needed." Speaking on a recent panel at conference hosted by the Bank for International Settlements (BIS), Chair Powell again noted that cryptocurrencies have been used for "illicit activity," adding that "we need to prevent this so that the innovations that do survive and do attract broad adoption are those that provide value over time."*

"" "Monetary Policy and the State of the Economy," U.S. House Financial Services Committee hearing, March 2, 2022; "Powell: Digital currencies will require new regulations," Associated Press, March 23, 2022.*

Cybersecurity Considerations

The Administration also released a statement and related Fact Sheet warning of the potential for Russia to engage in cyber-attacks on U.S. companies and the federal government technology infrastructure in response to imposed sanctions. The Administration urged companies to undertake a variety of measures to ensure resiliency and technological security, including to:

- Mandate multi-factor authentication to access systems
- Deploy modern security tools on devices
- Engage cybersecurity experts to protect against all known vulnerabilities, including changing passwords across networks
- Back up data and ensure offline backups are secure
- Run exercises and drill emergency plans to prepare for swift responses
- Encrypt data so it cannot be utilized by unauthorized users
- Educate employees on cybersecurity

Aligned with the Administration's releases, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has recommended all companies — regardless of size — adopt a heightened posture with regard to cybersecurity and the protection of critical assets and reiterated that companies can find resources and tools at Shields Up | CISA.

Please refer to:

- Treasury Press Release: U.S. Treasury Sanctions Russia's Defense-Industrial Base, the Russian Duma and Its Members, and Sberbank CEO
- White House Fact Sheet: United States and Allies and Partners Impose Additional Costs on Russia
- White House Fact Sheet: Act Now to Protect Against Potential Cyberattacks
- KPMG Regulatory Alert | U.S. Actions to Russia-Ukraine conflict
- KPMG Regulatory Alert | U.S. actions to Russia-Ukraine war: Expanded regulatory attentions
- KPMG Regulatory Alert | U.S. actions to Russia-Ukraine war: FinCEN Alert

For additional information, please contact Amy Matsuo, Steve Brotherton, John Caruso, or Matt Miller.

Contact the author:

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

kpmg.com/socialmedia