WINSTON & STRAWN LLP

BLOG

Russia–Ukraine Conflict Increases Regulatory Risks for Sanctions Evasion Through Crypto-Based Transactions

JULY 27, 2022

In response to Russia's invasion of Ukraine, the United States and dozens of its allies and partners around the globe have imposed what the White House has called "the most impactful, coordinated, and wide-ranging economic restrictions in history."[1] Although Russia is still not subject to a complete embargo in the United States, the sanctions placed on Russia have been severe and targeted against individuals and entities ("persons") operating in some of its most important sectors, such as the financial sector.[2] Under U.S. sanctions, for example, several key Russia-based financial institutions—including Russia's largest bank—and certain Russian elites (also known as "oligarchs") are now blocked, meaning their assets within the United States or in possession or control of U.S. Persons[3] are now "frozen." Furthermore, several top Russian banks have been banned from the Society for Worldwide Interbank Financial Telecommunication ("SWIFT")—a critical messaging system used by banks to make global payments. Such broad economic sanctions—in particular, those on Russia-based financial institutions—may heighten the risks for evasion through cryptocurrencies and other methods outside the traditional banking space.

On April 20, 2022, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") sanctioned (1) a Russian commercial bank and its subsidiary for suggesting sanctions-evasion techniques to its clients, including offering a SWIFT-alternative communication channel to process U.S. dollar payments to sanctioned entities; (2) more than 40 persons across the globe described as a "worldwide sanctions evasion and malign influence network" acting on behalf of a previously designated oligarch to evade sanctions; and (3) a virtual currency mining company for "operating or having operated in the technology sector of the Russian Federation economy."[4] In addition, over the past few months, OFAC, the Department of Commerce, the Federal Reserve, and the Financial Crimes Enforcement Network ("FinCEN") have issued alerts regarding Russian sanctions evasion, many of which note the use of cryptocurrencies as a part of such schemes.

Because U.S. Persons are broadly prohibited from engaging in transactions with sanctioned parties, and as sanctions are "strict liability," sanctions evasion not only presents designation risks for the evaders and facilitators but also presents risks of enforcement action (financial penalties), and practical and reputational risks to unwitting persons that process such payments. Considering the heightened risk of Russia sanctions evasion—including through the use of cryptocurrencies—financial institutions, crypto markets and exchanges, and other persons and individuals subject to U.S. jurisdiction or doing business with U.S. Persons, should consider implementing enhanced due diligence and/or taking extra precautions to avoid prohibited transactions or parties.

This article (1) provides an overview of OFAC sanctions jurisdiction and circumvention prohibitions, (2) summarizes recent Russia sanctions, (3) provides a synopsis re sanctions evasion through cryptocurrency, (4) highlights existing U.S. regulatory guidance regarding sanctions evasion through cryptocurrencies, and (5) recommends measures that persons and companies may wish to consider to mitigate the risk of sanctions violations.

1. OFAC Sanctions Jurisdiction and Prohibited Circumvention

OFAC has jurisdiction over all U.S. Persons, which under Executive Order 14024, Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation ("EO 14024"), includes "any United States citizen, lawful permanent resident, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States."[5] In addition, U.S. Persons generally are prohibited from approving, financing, facilitating, or guaranteeing any transaction by a foreign person where the transaction would be prohibited if performed by a U.S. person or within the United States.[6] Furthermore, non-U.S. Persons can be brought within OFAC's jurisdiction when there is some U.S. nexus to the transaction or where they cause U.S. Persons to violate sanctions. Finally, any transaction that circumvents sanctions or attempts to circumvent sanctions—i.e., that "evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate" the prohibitions, and "any conspiracy formed to violate" the prohibitions—also is prohibited and considered a separate violation.[7]

OFAC's jurisdiction is broad and, *even absent U.S. touchpoints on a transaction*, there are sanctions risks for non–U.S. Persons in engaging in activities with sanctioned persons. For example, non–U.S. Persons may be sanctioned for materially assisting, sponsoring, or providing financial, material, or technological support for, or goods or services to or in support of, blocked persons.[8] EO 14024 also authorizes sanctions on non-U.S. Persons for circumvention activities and attempts—e.g., any person directly or indirectly engaged in, or having attempted to engage in, deceptive or structured transactions or dealings to circumvent any United States sanctions, (including through the use of digital currencies or assets or the use of physical assets) for, on behalf of, or for the benefit of the Government of the Russian Federation.[9]

2. Russia Sanctions Overview

The United States and over 30 of its allies and partners have imposed sanctions on Russia in response to Russia's invasion of Ukraine.[10] As a part of such efforts, several Russian banks have been banned from the SWIFT network, which is a messaging system widely used by traditional banks and others in making global payments. In the United States alone, the U.S. government undertook several actions with respect to Russia, including, but not limited to, imposing blocking sanctions on important Russian banks, political figures, and oligarchs; certain debt and equity restrictions relating to several major firms; restrictions on Russian sovereign debt and entities critical to managing one of Russia's key sovereign wealth funds; prohibitions related to transactions involving the Central Bank of the Russian Federation, the National Wealth Fund of the Russian Federation, and the Ministry of Finance of the Russian Federation; certain import and export prohibitions; a prohibition on "new investments" in Russia; and more. Winston & Strawn has previously provided information on these sanctions in blogs published on March 28, 2022 and May 13, 2022.

OFAC's "blocking sanctions" are the strongest form of sanction. When OFAC designates a person under such sanctions, they are identified as a Specially Designated National ("SDN") or "blocked person" and listed on OFAC's List of Specially Designated Nationals and Blocked Persons (the "SDN List"). As a result, all of that person's property, and interests in property, that is in the United States or in the possession or control of U.S. Persons is blocked, i.e., frozen—and typically in an interest-bearing account; however, OFAC has special guidance for blocking digital-currency transactions.[11] In addition, under OFAC's 50 Percent Rule, any entities that are owned, directly or indirectly, 50% or more by an SDN/blocked person, whether individually or in the aggregate, are also considered blocked. As a result of the blocking requirement, U.S. Persons are prohibited from dealing with the blocked person in any way—including the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any blocked person and the receipt of any contribution or provision of funds, goods, or services from any such person.[12]

OFAC has designated hundreds of non–U.S. Persons as SDNs over the past few months for engaging in conduct for or on behalf of sanctioned persons and/or for evading Russia sanctions. Most recently, on April 20, 2022, OFAC sanctioned (1) a Russian commercial bank and its subsidiary for suggesting sanctions-evasion techniques to its clients, including offering a SWIFT-alternative communication channel to process U.S. dollar payments to sanctioned entities; (2) more than 40 persons across the globe described as a "worldwide sanctions evasion and malign influence network" acting on behalf of a previously designated oligarch to evade sanctions; and (3) a virtual currency mining company for "operating or having operated in the technology sector of the Russian Federation economy."[13] Notably, the virtual currency mining company was not expressly designated for evasion; however, OFAC noted that while Russia has a "comparative advantage in crypto mining due to energy resources and a cold climate," "mining companies rely on imported computer equipment and fiat payments, which makes them vulnerable to sanctions."[14] In the press release, OFAC noted that "[t]he United States is committed to ensuring that no asset, no matter how complex, becomes a mechanism for the Putin regime to offset the impact of sanctions."[15]

3. Sanctions Evasion Through Cryptocurrencies

Sanctions evasion is not just a cryptocurrency problem. Evasion techniques such as "wire stripping" to remove sanctioned-country information from wire transfer details have been occurring for decades. Even within the Russia context, OFAC confirms that "[s]anctioned Russian persons are known to employ a wide variety of measures in their efforts to evade U.S. and international sanctions" and alerts U.S. Persons that process or facilitate gold-related transactions to be vigilant due to circumvention risks.[16] The problem has also been recognized by international parties—a "Red Alert" issued by the UK National Crime Agency, National Economic Crime Centre, and HM Treasury Office of Financial Sanctions Implementation noted that "it is likely that DPs [Designated Persons] will explore alternative payment methods, including the use of crypto-assets, to move funds to circumvent sanctions and mitigate reduced access to the SWIFT payment system."[17]

In addition, using cryptocurrency to evade sanctions is not a newfound fear as a result of Russia's invasion of Ukraine. For example, several years ago, Venezuela's creation of the "petro" digital currency sparked conversation and concern regarding its use to evade sanctions, ultimately resulting in a March 2018 Executive Order prohibiting U.S. Persons from dealing in Venezuela-related digital coins and tokens.[18] Likewise, on May 6, 2022, OFAC sanctioned virtual currency mixer Blender.io ("Blender"), which "indiscriminately facilitate[d] illicit transactions by obfuscating their origin, destination, and counterparties" and was used by North Korea to launder over US$20 million in stolen virtual currency from a sanctioned state-sponsored cyber-hacking group's US$620 million virtual currency heist.[19]

Although certain actors may exploit cryptocurrencies to evade sanctions, it is not clear how often that has occurred thus far. For example, a Congressional Research Service report from February 2018 stated, "According to Treasury officials, . . . sanctions evasion risks posed by virtual currencies have been limited in practice."[20] Just last month, the FinCEN reported that it had "not seen widespread evasion of [U.S.] sanctions using methods such as cryptocurrency."[21]

Nonetheless, the U.S. government appears to be hyper-focused on controlling the space and prosecuting persons that evade sanctions using cryptocurrencies. For example, even prior to Russia's invasion of Ukraine, U.S. regulatory talking heads criticized the use of cryptocurrencies as a sanctions-evasion tool.[22] Furthermore, in October 2020, the DOJ's Cyber Digital Task Force published its Cryptocurrency Enforcement Framework,[23] in which the DOJ stated that "cryptocurrency presents a troubling new opportunity for individuals and rogue states to avoid international sanctions and to undermine traditional financial markets, thereby harming the interests of the United States and its allies."[24]

Since Russia's invasion of Ukraine, the U.S. government has continued to pick up speed and build efforts to enforce sanctions and control sanctions evasion. For example, only six days after Russia's invasion of Ukraine, Attorney General Merrick B. Garland announced the launch of an interagency law enforcement group—Task Force KleptoCapture—"dedicated to enforcing the sweeping sanctions, export restrictions, and economic countermeasures that the United States has imposed, along with allies and partners, in response to Russia's unprovoked military invasion of Ukraine."[25] Among other items, the "mission" of the task force includes "[t]argeting

efforts to use cryptocurrency to evade U.S. sanctions, launder proceeds of foreign corruption, or evade U.S. responses to Russian military aggression."[26] The same day, U.S. Senators Elizabeth Warren, Mark Warner, Sherrod Brown, and Jack Reed sent a letter to the Secretary of the Treasury expressing concerns about the sanctions enforcement challenges for digital-asset transactions, specifically citing the growing magnitude of transactions in cryptocurrencies, the decentralized nature of the assets, the policies and statements of various U.S. agencies, and other factors. The letter requested information on Treasury's plans to enforce U.S. laws and sanctions related to cryptocurrency, including working with foreign governments and the international banking community, specific enforcement challenges, new issues related to decentralized finance, and specific needs for enforcement.[27] Finally, in May, a federal magistrate judge in the United States District Court for the District of Columbia issued an unsealed opinion which revealed that the DOJ may be criminally prosecuting a U.S. Person for evading sanctions via cryptocurrency, including potentially Russia sanctions, among others.[28] This case has been described as "the first U.S. criminal prosecution targeting solely the use of cryptocurrency in a sanctions case."[29]

4. Existing Guidance for Financial Institutions and Crypto-Related Companies re Russia Sanctions Evasion via Crypto

As noted above, U.S. sanctions apply to *all* U.S. Persons—whether individuals or companies—regardless of the industry or business type. In addition, sanctions are strict liability, meaning there is no knowledge requirement, and even persons that accidentally or unknowingly engage in transactions with prohibited parties—such as SDNs—may be subject to enforcement action including financial penalties and reputational risks. This is particularly a concern with respect to recent U.S. sanctions on Russia (1) due to Russia's presence in the world market, including the fact that many U.S. Persons had operations or business in Russia, and (2) as the sanctions have been swift, robust, and complex.

Considering the heightened risk of Russia sanctions evasion—including through the use of cryptocurrencies—financial institutions, crypto markets and exchanges, and other persons and individuals subject to U.S. jurisdiction or doing business with U.S. Persons should consider taking extra precautions to avoid prohibited transactions or parties. That said, Treasury has thus far published only a few items with respect to this matter:

- Although not specifically related to Russian sanctions evasion, in October 2021 OFAC published its "Sanctions Compliance Guidance for the Virtual Currency Industry," stating that the "virtual currency industry, including technology companies, exchangers, administrators, miners, wallet providers, and users, plays an increasingly critical role in preventing sanctioned persons from exploiting virtual currencies to evade sanctions and undermine U.S. foreign policy and national security interests." This guidance document may be helpful for virtual currency entities that are generally new to the sanctions space.
- OFAC also issued an FAQ on March 11, 2022, stating that "sanctioned Russian persons are known to employ a wide variety of measures in their efforts to evade U.S. and international sanctions" and reminding U.S. Persons, "including firms that process virtual currency transactions," to "be vigilant against attempts to circumvent OFAC regulations and [that they] must take risk-based steps to ensure they do not engage in prohibited transactions."[30] The FAQ emphasizes that OFAC regulations apply to U.S. Persons wherever located, including those involved in or undertaking virtual currency transactions. That said, this FAQ is clearly more of an alert than practical guidance.
- On March 7, 2022, FinCEN issued an alert advising all financial institutions to be vigilant against attempts to evade economic sanctions and other U.S.-imposed restrictions related to the Russian invasion of Ukraine.[31] FinCEN noted in its alert that "sanctioned Russian and Belarusian actors may seek to evade sanctions through various means, including through non-sanctioned Russian and Belarusian financial institutions and financial institutions in third countries" and that "[s]anctions evasion activities could be conducted by a variety of actors, including CVC exchangers and administrators within or outside Russia, that retain at least some access to the international financial system."[32] FinCEN's alert provides examples of red flags for sanctions-evasion attempts, including sanctions-evasion attempts using CVC such as (1) transactions initiated from high-risk IP addresses, including from locations in Russia, (2) transactions connected to CVC addressed on OFAC's SDN List, and (3) a customer using a CVC exchanger or foreign-located money services business in a high-risk jurisdiction.

5. Compliance Tips to Consider

Although there have been several warnings about Russia sanctions evasion using cryptocurrencies, the guidance for U.S. Persons has been fairly limited. That said, there are a few things U.S. Persons can actively do to avoid engaging in a sanctions violation, including cryptocurrency-related sanctions-evasion transactions:

- **Take a "Risk-Based Approach" to Compliance.** As noted, OFAC sanctions are strict liability. U.S. companies, non-U.S. companies doing business in the United States, and those otherwise aiming to comply with OFAC sanctions are strongly encouraged to employ a "risk-based" sanctions compliance program that is tailored to meet the company's size, geographic areas of operation, products, services, customers, and counterparties. This means accounting for the unique aspects of cryptocurrencies, detecting and reporting suspicious activity, and minimizing the risk of cryptocurrency-related sanctions violations.
- **Meet the Elements for an Effective Sanctions Compliance Program.** OFAC's Framework for Compliance Commitments lists five essential elements of an effective sanctions compliance program: (1) management commitment, (2) a risk assessment, (3) internal controls, (4) testing and auditing, and (5) training. The Framework expands on each of these areas and should be considered accordingly.
- **"Know Your Customer."** Even if you are not engaged in business as a financial institution, companies dealing in cryptocurrency and other digital assets should prioritize strong know-your-customer ("KYC") procedures. In understanding who your customer is, you will better be able to identify unusual activity that may be indicative of sanctions evasion.
- **Collect Beneficial Owner Information.** Given OFAC's 50 Percent Rule, if a company is owned 50% or more by an SDN, whether individually or in the aggregate, it will be blocked. Delving into ownership information can be a complicated task given complex ownership structures commonly found within Russian entities.
- **Look to FinCEN's March 2020 Alert.** Again, even non-financial institutions may benefit from FinCEN's March 2020 alert regarding sanctions evasion. Several red flags provided may be helpful, applicable, or otherwise instructive to your company's business.
- **Reach out to us!** Russia sanctions can be extremely complicated and nuanced. We are here to help with all of your sanctions and crypto-related compliance needs.

Winston & Strawn continues to monitor the quickly changing situation with an interdisciplinary group of lawyers with expertise in trade, sanctions, financial services, and cryptocurrency, and will continue to provide updates and client alerts on new developments. If you would like to be added to our mailing list for client alerts or have questions about specific transactions, please contact the authors or your Winston relationship partner.

---

[1] The White House, FACT SHEET: United States, G7 and EU Impose Severe and Immediate Costs on Russia (Apr. 6, 2022), https://www.whitehouse.gov/briefing-room/statements-releases/2022/04/06/fact-sheet-united-states-g7-and-eu-impose-severe-and-immediate-costs-on-russia/.

[2] Dep't of Treasury, Press Releases: Treasury Targets Sanctions Evasion Networks and Russian Technology Companies Enabling Putin's War (Mar. 31, 2022), https://home.treasury.gov/news/press-releases/jy0692.

[3] Defined under Russia-related executive orders to include any United States citizen, lawful permanent resident, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or person in the United States. *See, e.g.*, Exec. Order 14024, Blocking Property With Respect To Specified Harmful Foreign Activities of the Government of the Russian Federation, 86 Fed. Reg. 20249 (Apr. 18, 2021).

[4] Dep't of Treasury, Press Releases: U.S. treasury Designates Facilitators of Russian Sanctions Evasion (Apr. 20, 2022), https://home.treasury.gov/news/press-releases/jy0731.

[5] *See, e.g.*, Exec. Order 14024, *supra* note 3.

[6] *See* Dep't of Treasury, Frequently Asked Questions 497 (Jan. 12, 2017), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/497.

[7] Exec. Order 14024, *supra* note 3, § 4.

[8] *Id.* § 1(a)(vi)(B).

[9] *Id.* § 1(a)(ii)(G).

[10] The White House, *supra* note 1.

[11] *See* Dep't of Treasury, Frequently Asked Questions 646 (Oct. 15, 2021), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/646.

[12] *See, e.g.,* Exec. Order 14024, *supra* note 3, § 1.

[13] Dep't of Treasury, *supra* note 4.

[14] *See id.*

[15] *See id.*

[16] *See* Dep't of Treasury, Frequently Asked Questions 1029 (June 28, 2022), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1029.

[17] Nat'l Crime Agency et al., Red ALERT: Financial Sanctions Evasion Typologies: Russian Elites and Enablers 4 (July 2022), https://www.nationalcrimeagency.gov.uk/who-we-are/publications/605-necc-financial-sanctions-evasion-russian-elites-and-enablers/file.

[18] Exec. Order No. 13827, 83 Fed. Reg. 12469 (Mar. 21, 2018).

[19] *Id.*

[20] Congressional Research Service, Digital Currencies: Sanctions Evasion Risks 1–3 (Feb. 8, 2018), https://crsreports.congress.gov/product/pdf/IF/IF10825/3.

[21] Dep't of Treasury, FinCEN Provides Financial Institutions With Red Flags on Potential Russian Sanctions Evasion Attempts (Mar. 7, 2022), https://www.fincen.gov/news/news-releases/fincen-provides-financial-institutions-red-flags-potential-russian-sanctions#:~:text=%E2%80%9CAlthough%20we%20have%20not%20seen,support%20Ukraine%20and%20its%20people.%E2%80%9D.

[22] For example, SEC Chair Gary Gensler said that "[t]o the extent that [cryptocurrency] is used as [a medium of exchange], it's often to skirt our laws with respect to … sanctions." Chair Gary Gensler, Remarks Before the Aspen Security Forum (Aug. 3, 2021), https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03.

[23] Dep't of Just., Cryptocurrency Enforcement Framework (Oct. 2020), https://www.justice.gov/archives/ag/page/file/1326061/download.

[24] *Id.* at 51–52.

[25] Dep't of Just., Attorney General Merrick B. Garland Announces Launch of Task Force KleptoCapture (Mar. 2, 2022), https://www.justice.gov/opa/pr/attorney-general-merrick-b-garland-announces-launch-task-force-kleptocapture.

[26] *See id.*

[27] Elizabeth Warren, Mark R. Warner, Letter to Janet Yellen (Mar. 2, 2022), https://www.warren.senate.gov/imo/media/doc/2022.03.01%20Letter%20to%20Treasury%20re%20OFAC%20crypto%20sanctions%20enforcement.pdf.

[28] *In re Crim. Complaint*, No. 22-MJ-067-ZMF, 2022 WL1573361 (D.D.C. May 13, 2022), https://www.dcd.uscourts.gov/sites/dcd/files/22mj00067CriminalOpinion.pdf.

[29] Spencer S. Hsu, *U.S. Issues Charges in First Criminal Cryptocurrency Sanctions Case*, Wash. Post (May 16, 2022), https://www.washingtonpost.com/dc-md-va/2022/05/16/first-us-criminal-cryptocurrency-sanctions/.

[30] Dep't of Treasury, Frequently Asked Questions 1021 (Mar. 11, 2022), https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1021.

[31] Dep't of Treasury, *supra* note 21.

[32] *Id.* at 2.

10+ Min Read

Authors

Cari Stinebower

Dainia Jabaji

Jacob Harding

Related Locations

Los Angeles | Washington, DC

Related Topics

Russia | Ukraine | Sanctions | Anti-Money Laundering (AML) | Financial Services and Banking | Cryptocurrency

Related Capabilities

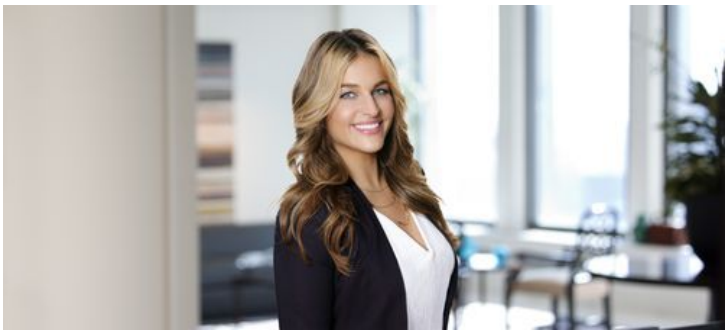
Tax | Maritime & Admiralty | Financial Services | Cryptocurrencies, Digital Assets & Blockchain Technology

Related Regions

North America

Related Professionals

Cari Stinebower



Dainia Jabaji

Jacob Harding

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.