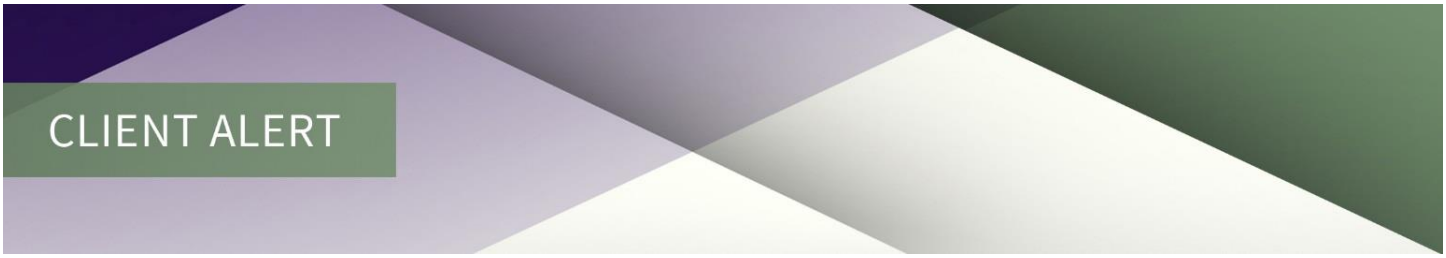

Will Crypto Make a Hash of the Sanctions Against Russia? Sanctions Evasion Considerations for the Cryptocurrency Sector

March 21, 2022

AUTHORS

Britt Mosman | J. Christopher Giancarlo | Conrad G. Bahlke | Justin L. Browder
Artyom Rogov | Michael J. Passalacqua

The United States and its allies have responded to Russia's invasion of Ukraine by imposing severe and unprecedented sanctions that isolate Russian-based financial institutions, President Putin and certain of his associates, and certain regions of Russia and Ukraine from the global financial and trade system. The sanctions measures, which we discuss in detail in prior Client Alerts,[1] include sweeping financial sanctions that have had a profound impact on Russia's economy and financial system. As a result, certain features of cryptocurrencies and their underlying technologies, such as the ease of transferability, transaction anonymity, and decentralization may initially appear to make the asset class attractive to persons that are blocked from the traditional U.S. financial system.

These developments have led many to ask, to what extent can cryptocurrency be used to evade Russia sanctions?

This alert addresses the potential use of cryptocurrency to circumvent sanctions on Russia and provides recommendations to crypto-sector participants to aid compliance with U.S. sanctions prohibitions. Although large-scale sanctions evasion using cryptocurrency by the Russian government may well not be practicable, for the reasons

[1] Please see Willkie client alerts "State of Play: U.S. Sanctions Against Russia for the Crisis in Ukraine," "In a Parallel Rollout, the US, EU, and UK Sanction Major Russian Financial Institutions and Russian Sovereign Debt and Take Additional Measures," "United States Escalates Sanctions Against Russia, Targeting Major Russian Financial Institutions and Russian President Vladimir Putin" and "In First Response to Russian Intervention in Ukraine, President Biden Imposes Comprehensive Sanctions on the Donetsk and Luhansk Regions of Ukraine."

discussed herein, there is concern among some U.S. policymakers that sanctioned persons in Russia will turn to cryptocurrency as they become more desperate for access to the global financial system. However, the design of many cryptocurrencies, including Bitcoin and Ether, is such that cryptocurrency holdings and transactions generate significant amounts of publicly available data that make it possible in many circumstances for centralized cryptocurrency exchanges to detect potential illicit activity and prevent persons located in certain geographical regions or persons targeted by sanctions (collectively, "**Sanctions Targets**") from converting cryptocurrencies into fiat currency. These exchanges are critical in the cryptocurrency ecosystem as they provide on-and-off ramps between cryptocurrencies and fiat currency. Thus, if exchanges prevent Sanctions Targets from converting cryptocurrencies into fiat currency, then cryptocurrencies become a less attractive asset class for Sanctions Targets seeking to evade sanctions. That being said, the Treasury Department's Office of Foreign Assets Control ("**OFAC**") has made clear that preventing sanctions evasion through cryptocurrency is a high priority for the agency, and it intends to use its sanctions authorities to counter the use of cryptocurrencies by Sanctions Targets and other malicious actors who abuse cryptocurrencies and emerging payment systems.

Overview of U.S. Sanctions

As detailed in our prior Client Alert discussing sanctions considerations for the crypto-sector more generally, OFAC administers and enforces various economic sanctions programs against geographical regions, governments, groups, and individuals. OFAC regulations generally prohibit U.S. persons[2] from engaging in transactions, directly or indirectly, with Sanctions Targets. In addition, U.S. persons are generally prohibited from "facilitating" or assisting the actions of non-U.S. persons that would be prohibited for U.S. persons to perform directly due to U.S. sanctions. Under OFAC's definition of U.S. persons, cryptocurrency exchanges, technology companies, payment processers, and administrators located or organized in the United States are considered U.S. persons. In addition, any users of digital currencies who are U.S. citizens or "green card" holders, regardless of where such individuals are located, are U.S. persons under OFAC's definition. As a result, those persons are directly restrained by U.S. sanctions from providing benefits to a sanctioned jurisdiction or engaging in any transaction involving a designated person.

In the past few years, OFAC has increasingly designated persons that have used virtual currency in connection with malign activity, including several Russian persons. For example, in September 2021, OFAC designated SUEX OTC, S.R.O. ("**SUEX**"), a Russian virtual currency exchange, for facilitating financial transactions for ransomware actors. An analysis of SUEX transactions highlighted that over 40% of SUEX's known transaction history was associated with illicit

[2] U.S. persons are defined to include: (i) United States citizens and permanent resident aliens, wherever located; (ii) all entities organized in the United States (including their foreign branches); and (iii) all individuals, entities and organizations actually located in the United States. For the U.S. sanctions against Cuba and Iran, all entities owned or controlled by U.S. persons, wherever organized or doing business (including foreign subsidiaries), are also generally required to comply with such sanctions.

actors.[3] In addition, OFAC has designated various Russian entities associated with certain malware and malware-related cyberattacks, such as Evil Corp—the Russia-based cybercriminal organization behind the Dridex malware.[4]

More recently, the United States imposed comprehensive, territorial sanctions on the so-called Donetsk People's Republic ("**DNR**") and the Luhansk People's Republic ("**LNR**") regions of Ukraine. These sanctions, which closely mirror the comprehensive sanctions imposed on the Crimea region of Ukraine in 2014, broadly prohibit U.S. persons from engaging in virtually any transactions or dealings involving the DNR and LNR (directly or indirectly), unless exempt or authorized by OFAC.

Potential for Cryptocurrency to Evade Russia Sanctions

Some members of the U.S. government have expressed concern that cryptocurrencies may offer Sanctions Targets and other illicit actors an alternative means of facilitating transactions due to their ease of transferability, transaction anonymity, and decentralization features. These concerns have become even more urgent given the sanctions imposed on Russia after its invasion of Ukraine and reports that "Russian entities are preparing to blunt some of the worst effects" of the sanctions that have been levied on the country by using the array of "cryptocurrency-related tools at its disposal."[5] Indeed, Russia's largest financial institution, Sberbank, reportedly just received a license from the Russian Central Bank to issue digital assets to clients, a significant departure from Russia's pre-war crypto stance.[6] A recent report prepared by the U.S. Treasury Department noted how technological innovations, such as cryptocurrencies, potentially reduce the efficacy of American sanctions since crypto transactions offer malign actors opportunities to hold and transfer funds outside the traditional dollar-based financial system.[7] In addition, on March 2, 2022, Senators Elizabeth Warren, Mark Warner, Sherrod Brown, and Jack Reed, wrote to U.S. Treasury Secretary Janet Yellen voicing concerns about the Treasury Department's progress in monitoring and enforcing sanctions compliance within the cryptocurrency industry, especially given the need to ensure the efficacy and integrity of U.S. sanctions against Russia.[8]

However, these concerns may not be as widespread as initial reports suggested. On March 8, 2022, during a background press conference on President Biden's recent executive order on the responsible development of digital assets, a senior Biden Administration official, when asked about the topic of sanctions, stated: "[On] Russia, in particular, the use of

---

3 *Id*.

4 Department of the Treasury, Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, Sep. 21, 2021, available here.

5 Emily Flitter and David Yaffe-Bellany, Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions, The New York Times, Feb. 23, 2022, available here.

6 Will Daniel, Russian banks are so broke the biggest lender just got the go-ahead to issue digital assets like crypto, Fortune, Mar. 18, 2022, available here.

7 Department of the Treasury, The Treasury 2021 Sanctions Review, Oct. 2021, available here.

8 United States Senate, Letter to Treasury re OFAC crypto sanctions enforcement, Mar. 2, 2022, available here.

cryptocurrency we do not think is a viable workaround to the set of financial sanctions we've imposed across the entire Russian economy and, in particular, to its central bank."[9] Moreover, according to Carole House, Director of Cybersecurity and Secure Digital Innovation for the National Security Council, the scale that the Russian state would need to successfully circumvent all U.S. and partners' financial sanctions would almost certainly render cryptocurrency as an ineffective primary tool for the state.[10] In addition, Acting Director of the U.S. Treasury Department's Financial Crimes Enforcement Network ("**FinCEN**"), Him Das, commented on the potential for Russia to evade sanctions by the use of cryptocurrencies, stating: "[a]lthough we have not seen widespread evasion of our sanctions using methods such as cryptocurrency, prompt reporting of suspicious activity contributes to our national security and our efforts to support Ukraine and its people."[11]

To further explore the use of cryptocurrencies surrounding sanctions, the Senate Banking Committee held a hearing on March 17, 2022, titled Understanding the Role of Digital Assets in Illicit Finance.[12] During the hearing, Senator Warren announced the introduction of a new bill titled the Digital Asset Sanctions Compliance Enhancement Act of 2022, which would "combat the risk of Russian actors from using digital assets to evade international sanctions by discouraging foreign crypto firms from doing business with sanctioned Russian elites, providing the Administration with authority to suspend transactions with Russia-linked crypto addresses, and increasing transparency around crypto holdings."[13] Specifically, the bill would provide the Treasury Secretary clear authority to prohibit digital asset trading platforms under U.S. jurisdiction from transacting with accounts known to be in Russia.[14] The bill would also require U.S. taxpayers who transact with a value greater than $10,000 in cryptocurrency outside the U.S. to file a FinCEN Form 114 and require the Treasury Department to issue a public report identifying foreign digital asset trading platforms that are considered high risk in terms of sanctions evasion, money laundering, and other illicit activities.[15] Importantly, not all participants at the hearing shared the same level of concern voiced by Senator Warren. For example, in the written statement prepared by Michael Mosier, Former Acting Director, Deputy Director/Digital Innovation Officer of FinCEN, he referenced a remark made by Counselor

9 Press Briefing, Background Press Call by Senior Administration Officials on the President's New Digital Assets Executive Order, Mar. 8, 2022, available here.

10 Hannah Lang, U.S. lawmakers push Treasury to ensure Russia cannot use cryptocurrency to avoid sanctions, Reuters, Mar. 2, 2022, available here.

11 Immediate Release, FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts, Mar. 7, 2022, available here.

12 United States Senate Committee on Banking, Housing, and Urban Affairs, Understanding the Role of Digital Assets in Illicit Finance, 117th (2022).

13 Crypto Sanctions Bill One-Pager_3.16.22 final, Digital Asset Sanctions Compliance Enhancement Act of 2022, available here.

14 *Id*.

15 *Id*.

to the Deputy Secretary of the Treasury, Todd Conklin, which said, "[y]ou can't flip a switch overnight and run a G20 economy on cryptocurrency. It's an access problem, it's a rails problem, and it's just a basic liquidity problem."[16]

Executive Order on Ensuring Responsible Development of Digital Assets

In a related action, the White House issued an Executive Order on March 9, 2022 outlining the Biden Administration's approach to the crypto industry, entitled Executive Order on Ensuring Responsible Development of Digital Assets (the "**Order**"), which discussed the concern that cryptocurrency may be used as a tool to promote illicit finance and various other activities.[17] For a more detailed discussion on the Order, please visit our Client Alert.

The Order calls for action from nearly all of the Federal financial regulators, various departments of the U.S. Cabinet (including Treasury, State, Justice, and others), the Office of Science and Technology Policy, the Director of National Intelligence, and a number of other agencies and officials to help mitigate the illicit finance and national security risks resulting from the misuse of cryptocurrencies.[18] These risks include (among others) the risk that cryptocurrencies may be the means by which Sanctions Targets circumvent U.S. and foreign sanctions regimes. For example, the Order notes that illicit actors often launder and cash-out their illicit proceeds using cryptocurrency service providers, such as cryptocurrency exchanges, in jurisdictions that have not yet effectively implemented the international standards set by the Financial Action Task Force ("**FATF**").[19] Therefore, the continued availability of service providers in such jurisdictions supports financial activity without illicit finance controls.[20]

The Order briefly addresses an additional concern related to the decentralized finance ecosystem and peer-to-peer payments, which may be additional avenues for illicit finance activities.[21] The Order notes that when cryptocurrencies are misused, there is a significant threat to the national security of the United States, and calls on numerous agencies to provide a report devising a plan for mitigating crypto-specific illicit finance and national security risks while preserving the efficacy of the United States' national security tools.[22]

---

16 Testimony of Michael Mosier Before the United States Senate Committee on Banking, Housing, and Urban Affairs, "Understanding the Role of Digital Assets in Illicit Finance," Mar. 17, 2022, available here.

17 Statements and Releases, FACT SHEET: President Biden to Sign Executive Order on Ensuring Responsible Development of Digital Assets, Mar. 9, 2022, available here, and Presidential Actions, Executive Order on Ensuring Responsible Development of Digital Assets, Mar. 9, 2022, available here.

18 *Id*.

19 *Id*.

20 *Id*.

21 *Id*.

22 *Id*.

Sanctions Compliance Recommendations

As Sanctions Targets in Russia and in the Crimea, DNR, and LNR regions of Ukraine become more desperate for access to the U.S. financial system, it is important for crypto-sector participants to prioritize the implementation and maintenance of effective sanctions compliance controls to mitigate the risk of Sanctions Targets exploiting cryptocurrencies to undermine U.S. foreign policy interests and national security. To that end, FinCEN has issued an alert outlining certain transactional red flags for cryptocurrency market participants to help them identify potential sanctions evasion efforts.

These red flags include when:

- A customer's transactions are initiated from or sent to the following types of IP addresses: non-trusted sources; locations in Russia, Belarus, FATF-identified jurisdictions with AML/CFT/CP deficiencies, and comprehensively sanctioned jurisdictions; or IP addresses previously flagged as suspicious;
- A customer's transactions are connected to cryptocurrency addresses listed on OFAC's Specially Designated Nationals and Blocked Persons List (the "**SDN List**"); or
- A customer uses a cryptocurrency exchange or foreign-located money services business in a high-risk jurisdiction with AML/CFT/CP deficiencies, particularly for cryptocurrency entities and activities, including inadequate "know-your-customer" or customer due diligence measures.[23]

Given the sanctions-related risks we have discussed above, we recommend the following basic steps (at a minimum) for U.S. participants in the cryptocurrency industry:

- Develop and implement a sanctions compliance program that incorporates each of the five core elements of compliance discussed in OFAC's Framework for OFAC Compliance Commitments:[24] (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training;
- Screen the digital addresses, names, locations, and identifying information of all incoming and outgoing transactions. The frequency of screening will depend on the business's risk profile, but in our view, should generally occur at account opening and periodically thereafter. It may be prudent to conduct enhanced screening of transactions involving Russia as well as any region in which a high concentration of SDNs are designated;

[23] FinCEN Alert, FinCEN Advises Increased Vigilance for Potential Russian Sanction Evasion Attempts, Mar. 7, 2022, available here.

[24] U.S. Department of the Treasury, A Framework for OFAC Compliance Commitments, May 29, 2019, available online here.

- Identify (depending on the U.S. person's risk profile) red flags that indicate that a blocked person may continue to have an interest in a digital asset, regardless of how many times the asset is transferred away from a known blocked address;

- Develop procedures to prevent transactions involving blocked coins (such as the Petro). For example, if the "digital ruble" (the digital currency of the Russian Central Bank that is currently in a pilot phase) becomes blocked, then U.S. persons would be prohibited from engaging in any transactions involving it;

- Block transactions involving IP addresses, physical addresses, and other identifiers that appear to originate in sanctioned jurisdictions, including Crimea, the DNR, and the LNR regions of Ukraine; and

- Consider the use of address-clustering software and other blockchain analytics tools, where practicable, to identify addresses associated with blocked addresses that are not on the SDN List.

Over the past few weeks, the sanctions that have been imposed against Russia represent unprecedented diplomatic and economic costs to Russia. In the face of mounting economic pressure on Russia, and in light of the sanctions that have isolated it from the global financial system, U.S. persons should be vigilant about potential Russian sanctions evasion by taking the steps recommended herein.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Britt Mosman
202 303 1057
bmosman@willkie.com

J. Christopher Giancarlo
212 728 3816
jcgiancarlo@willkie.com

Conrad G. Bahlke
212 728 8233
cbahlke@willkie.com

Justin L. Browder
202 303 1264
jbrowder@willkie.com

Artyom Rogov
212 728 8744
arogov@willkie.com

Michael J. Passalacqua
212 728 8329
mpassalacqua@willkie.com