

United States Senate
WASHINGTON, DC 20510

March 2, 2022

The Honorable Janet Yellen
Secretary
Department of the Treasury
1500 Pennsylvania Avenue NW
Washington, DC 20220

Dear Secretary Yellen:

We write to inquire about the Treasury Department's progress in monitoring and enforcing sanctions compliance by the cryptocurrency industry and to express our concern that criminals, rogue states, and other actors may use digital assets and alternative payment platforms as a new means to hide cross-border transactions for nefarious purposes. Recent reports, including the Department's *2021 Sanctions Review*, have warned that such digital assets and alternative payment platforms may facilitate evasion of U.S. and global sanctions, potentially undermining the efficacy of our sanctions regime.¹ 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 as its disposal."² Given the need to ensure the efficacy and integrity of our sanctions program against Russia and other adversaries, we are seeking information on the steps Treasury is taking to enforce sanctions compliance by the cryptocurrency industry.

The cryptocurrency industry has seen tremendous growth in recent years, with its market capitalization roughly tripling in 2021 to reach nearly \$3 trillion.³ Recognizing the rapid growth of the market, Treasury's Office of Foreign Assets Control (OFAC) released its "Sanctions Compliance Guidance for the Virtual Currency Industry" in October 2021.⁴ As the guidance notes, "The growing prevalence of virtual currency as a payment method likewise brings greater exposure to sanctions risks—like the risk that a sanctioned person or a person in a jurisdiction subject to sanctions might be involved in a virtual currency transaction."⁵ The guidance outlines

¹ Department of Treasury, "The Treasury 2021 Sanctions Review," October, 2021, <https://home.treasury.gov/system/files/136/Treasury-2021-sanctions-review.pdf>; <https://s.wsj.net/public/resources/documents/unpanelofexperts.pdf>.

² The New York Times, "Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions," Emily Flitter and David Yaffe-Bellany, February 23, 2022, <https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html>.

³ Bloomberg, "Crypto Barrels Toward 2022 After Adding \$1.5 Trillion In Value," Akshay Chinchalkar, December 20, 2021, <https://www.bloomberg.com/news/articles/2021-12-20/cryptocurrencies-and-bitcoin-btc-2021-year-in-charts>.

⁴ Office of Foreign Assets Control, "Sanctions Compliance Guidance for the Virtual Currency Industry," October 2021, https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

⁵ *Id.*

best practices for compliance and makes clear that all actors in the cryptocurrency space, including “technology companies, exchangers, administrators, miners, wallet providers, and users,” are “responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions.”⁶

Strong enforcement of sanctions compliance in the cryptocurrency industry is critical given that digital assets, which allow entities to bypass the traditional financial system, may increasingly be used as a tool for sanctions evasion. In a February 2022 report, the United Nations found that North Korea used stolen cryptocurrency – worth perhaps as much as \$400 million – to fund its nuclear and ballistic missile program in contravention of international sanctions.⁷ A May 2021 report by the blockchain analytics firm Elliptic found that Iran has turned to bitcoin mining as “an attractive opportunity for a sanctions-hit economy suffering from a shortage of hard cash,” allowing it to “earn hundreds of millions of dollars in cryptocurrencies that can be used to buy imports and lessen the impact of sanctions.”⁸

In addition, there are growing concerns that Russia may use cryptocurrencies to circumvent the broad new sanctions it faces from the Biden administration and foreign governments in response to its invasion of Ukraine.⁹ This could include the use of dark web marketplaces that are powered by cryptocurrencies to move funds and conduct transactions; the use of crypto wallets and mixing services that allow sanctioned entities to transfer and hide their wealth; deployment of a digital ruble that would allow Russia to conduct foreign trade without converting their currency into dollars; and ransomware attacks that would allow Russian actors to recoup revenues lost to sanctions.¹⁰ Indeed, nearly three-quarters of all global ransomware revenue last year, or more than \$400 million in cryptocurrency payments, is estimated to have gone to Russia-affiliated entities.¹¹ Trading volumes between the Russian ruble and Bitcoin have spiked to their highest level since May 2021 in recent days following the wave of sanctions announcements.¹²

These reports are even more troubling because of analyses that suggest that the cryptocurrency industry may not be fulfilling its responsibility to comply with U.S. sanctions. OFAC’s October guidance notes that many “members of the virtual currency industry implement OFAC sanctions policies and procedures months, or even years, after commencing operations... expos[ing] virtual currency companies to a wide variety of potential sanctions risks.”¹³ When Marathon Digital, a crypto mining company, announced it would refuse to process transactions involving crypto

⁶ *Id.*

⁷ BBC, “North Korea: Missile programme funded through stolen crypto, UN report says,” February 6, 2022, <https://www.bbc.com/news/world-asia-60281129>.

⁸ Reuters, “Iran uses crypto mining to lessen impact of sanctions, study finds,” Anna Irrera, May 21, 2021, <https://www.reuters.com/technology/iran-uses-crypto-mining-lesser-impact-sanctions-study-finds-2021-05-21/>.

⁹ The New York Times, “Russia Could Use Cryptocurrency to Blunt the Force of U.S. Sanctions,” Emily Flitter and David Yaffe-Bellany, February 23, 2022, <https://www.nytimes.com/2022/02/23/business/russia-sanctions-cryptocurrency.html>.

¹⁰ *Id.*

¹¹ *Id.*

¹² Bloomberg, “Bitcoin Volume Spikes in Russia and Ukraine as Sanctions Hit,” Muyao Shen, February 28, 2022, <https://www.bloomberg.com/news/articles/2022-02-28/bitcoin-volume-spikes-in-russia-and-ukraine-as-sanctions-hit>.

¹³ Office of Foreign Assets Control, “Sanctions Compliance Guidance for the Virtual Currency Industry,” October 2021, https://home.treasury.gov/system/files/126/virtual_currency_guidance_brochure.pdf.

wallets that appeared on OFAC’s Specially Designated Nationals and Blocked Persons List,¹⁴ the company received backlash from the cryptocurrency community because, according to Marathon CEO Fred Thiel, some industry members are “against the whole concept of doing anything that has to do with financial regulatory compliance or government regulation.”¹⁵ Ultimately, Marathon terminated the sanctions-compliant arrangement under industry pressure.¹⁶

The growth of activity in the Decentralized Finance (DeFi) space of the cryptocurrency market raises additional concerns about sanctions compliance.¹⁷ DeFi aims to “eliminat[e] human intermediaries like brokers, bank clerks and traders, and instead uses algorithms to execute financial transactions.”¹⁸ Unlike traditional financial institutions, or even the larger, centralized cryptocurrency exchanges, DeFi protocols rarely apply Know Your Customer/Anti-Money Laundering screenings to the activity occurring on their platforms.¹⁹ To the extent any are conducting checks, they are reportedly “bare-bones.”²⁰ In 2021, DeFi protocols received nearly \$1 billion in value from illicit wallets, a nearly 2,000% increase from the previous year.²¹ In a recent report, the Financial Crimes Enforcement Network (FinCEN) cited DeFi as a means for bad actors, including ransomware attackers, to convert illicit proceeds.²²

In recent years, OFAC has become increasingly reliant upon voluntary self-disclosure from sanctions violators for enforcement, with one report concluding that 67% of enforcement cases during the Trump administration were prompted by self-disclosure.²³ However, this model appears to be particularly ill-suited for enforcing sanctions compliance in the cryptocurrency industry given the prevalence of pseudonymity and the current weakness of the industry’s compliance programs. Moreover, when OFAC has brought enforcement actions against cryptocurrency industry participants, it has generally accorded substantial deference to

¹⁴ CoinDesk, “Marathon Miners Have Started Censoring Bitcoin Transactions; Here’s What That Means,” Colin Harper, May 7, 2021, <https://www.coindesk.com/tech/2021/05/07/marathon-miners-have-started-censoring-bitcoin-transactions-heres-what-that-means/>.

¹⁵ The Block, “Marathon says its mining pool will stop censoring transactions following bitcoin community outcry,” Kollen Post, June 2, 2021, <https://www.theblockcrypto.com/linkedin/106865/marathon-ofac-bitcoin-mining-pool-taproot>.

¹⁶ *Id.*

¹⁷ Chainalysis, “DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate,” Chainalysis Team, January 26, 2022, <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/>.

¹⁸ The New York Times, “Crypto’s Rapid Move Into Banking Elicits Alarm in Washington,” Eric Lipton and Ephrat Livni, November 1, 2021, <https://www.nytimes.com/2021/09/05/us/politics/cryptocurrency-banking-regulation.html>

¹⁹ Decrypt, “Most Crypto Exchanges Have Weak KYC, DeFi is Making It Worse,” Drew Hutchinson, October 1, 2020, <https://decrypt.co/43486/crypto-exchanges-weak-kyc-defi-dex-report>; Financial Times, “Cryptocurrency: rise of decentralised finance sparks ‘dirty money’ fears,” Gary Silverman, September 15, 2021, <https://www.ft.com/content/bbeb2f8c-99ec-494b-aa76-a7be0bf9dae6>.

²⁰ Elliptic, “DeFi: Risk, Regulation, and the Rise of DeCrime,” November 18, 2021, <https://www.elliptic.co/resources/defi-risk-regulation-and-the-rise-of-decrime>.

²¹ Chainalysis, “DeFi Takes on Bigger Role in Money Laundering But Small Group of Centralized Services Still Dominate,” Chainalysis Team, January 26, 2022, <https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-cryptocurrency-money-laundering/>.

²² Financial Crimes Enforcement Network, “Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021,” October 15, 2021, <https://www.fincen.gov/news/news-releases/fincen-issues-report-ransomware-trends-bank-secrecy-act-data>.

²³ War on the Rocks, “The Past, Present, and Future of U.S. Sanctions Enforcement,” Bryan Early and Keith Preble, February 23, 2021, <https://warontherocks.com/2021/02/the-past-present-and-future-of-u-s-sanctions-enforcement/>.


mitigating factors in assessing penalties – even in cases where a company has not voluntarily self-disclosed apparent violations.²⁴ This approach has yielded penalties that are orders of magnitude below even the base civil monetary penalties for violations.²⁵ We are concerned that OFAC has not developed sufficiently strong and effective procedures for enforcement in the cryptocurrency industry.

To ensure that economic sanctions remain an effective tool for achieving our foreign policy goals, we ask that Treasury provide information on how it intends to enforce OFAC’s sanctions-compliance guidance for the cryptocurrency community and inhibit the use of cryptocurrency for sanctions evasion no later than March 23, 2022, including providing answers to the following questions:

1. How does OFAC work with foreign governments and other participants in the international banking community to ensure that cryptocurrency is not used to evade sanctions?
2. What are the challenges OFAC has faced in applying the October guidance?
3. Of all sanctions violations documented by OFAC in the virtual currency industry, what percentage of them were self-disclosed?
4. How has the growth of DeFi arrangements and services affected malign actors’ ability to circumvent sanctions, as well as OFAC’s ability to enforce sanctions?
5. What additional tools, including legal authorities or funding, might be necessary for OFAC to ensure that cryptocurrency participants are not able to help Russia or other malign actors evade U.S. and multilateral sanctions?

Thank you for your consideration.

Sincerely,


Elizabeth Warren
United States Senator

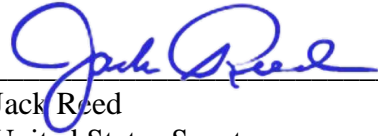

Mark R. Warner
United States Senator

²⁴ Department of Treasury, “OFAC Enters Into \$507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions,” Enforcement Release, February 18, 2021, https://home.treasury.gov/system/files/126/20210218_bp.pdf.

²⁵ *Id.*



Sherrod Brown
United States Senator



Jack Reed
United States Senator