National Security, Sanctions, and Export Controls

4 Key Questions Answered in OFAC's Guidance for the Virtual Currency Industry

By: Rachel K. Alpert, Shoba Pillay, and Emily A. Merrifield

Introduction

On October 15, 2021, the US Department of the Treasury's (Treasury) Office of Foreign Assets Control (OFAC) issued guidance to help the virtual currency industry navigate and comply with OFAC sanctions. The guidance improves on earlier FAQs by providing sanctions compliance best practices tailored for the virtual currency industry and reflects Treasury's commitment to "modernize and strengthen" US sanctions programs to adapt to what Treasury's October 18, 2021 report on the 2021 Sanctions Review described as "a changing world where financial innovation, shifts in global economic activity, and new geopolitical challenges are redefining how economic power can be used to support national security objectives." The straightforward, visual format of this guidance also exemplifies Treasury's renewed effort, as noted in the 2021 Sanctions Review report, to "enhance its public messaging" on sanctions and "improve public understanding of the intent and effect of sanctions."

This guidance follows closely on the heels of other US government actions related to the virtual currency industry. For example, the Department of Justice recently announced the National Cryptocurrency Enforcement Team, which will investigate and prosecute criminal use of cryptocurrency, focusing on criminal activity by cryptocurrency platform providers and money laundering infrastructure providers, as well as crimes using cryptocurrency platforms. Additionally, the SEC's chair, Gary Gensler, has made it clear that virtual currency issues will continue to be a priority for the SEC, and FinCEN has indicated an increased focus on cryptocurrency with the announcement in July 2021 of its first Chief Digital Currency Advisor after the January 2021 extension of the comment period of a proposed rule regarding certain transactions involving convertible virtual currency or digital assets with legal tender status.

Individuals and companies who interact with the virtual currency industry should be aware of the following four key answers from OFAC's new virtual currency guidance:

1. Who needs to be concerned about possible sanctions risks?

This guidance provides notice of sanctions risks to anyone associated with the virtual currency industry —including technology companies, exchangers, administrators, miners, wallet providers, and users, as well as more traditional financial institutions that may have exposure to virtual currencies or their service providers. All US persons are required to comply with OFAC regulations. This includes all US citizens and lawful permanent residents, wherever located; all individuals and entities within the United States; and all entities organized under the laws of the United States, including any foreign branches of those entities. Accordingly, anyone engaging in virtual currency activities in the United States, or that involve US individuals or entities, should be aware of OFAC sanctions requirements and take steps to comply.

2. What does OFAC mean by the following terms: "digital currency," "digital currency wallet," "digital currency address," and "virtual currency"?

• **Digital currency** includes sovereign cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat currency (e.g., Bitcoin).

• A **digital currency wallet** is a software application (or other mechanism) that provides a means

for holding, storing, and transferring digital currency (e.g., Coinbase).

• A **digital currency address** is an alphanumeric identifier that represents a potential designation for a digital currency transfer and is associated with a digital currency wallet (e.g., "Digital Currency Address – XBT").

• **Virtual currency** is a digital representation of value that functions as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; and is neither issued nor guaranteed by any jurisdiction (e.g., Bitcoin or Monero).

3. What should a US person do if they encounter sanctioned virtual currency?

Many OFAC sanctions programs require the blocking of any property or interests in property of sanctioned persons that is located in or comes within the United States or the possession or control of a US person. Once a US person determines that they hold virtual currency that is required to be blocked pursuant to OFAC's regulations, new OFAC FAQ 646 confirms that the US person must:

• Deny all parties access to that virtual currency;

• Ensure they comply with OFAC regulations relating to the holding and reporting of blocked assets;

• Implement controls that align with a risk-based approach; and

• Report the blocked virtual currency to OFAC within 10 business days, and thereafter on an annual basis, so long as the virtual currency remains blocked.

OFAC's guidance further clarifies that US persons are not obligated to convert the blocked virtual currency into traditional fiat currency (e.g., US dollars) and are not required to hold such blocked property in an interest-bearing account, as is generally required for blocked property.

4. What are sanctions compliance best practices in the virtual currency industry?

• Evaluate sanctions risks early, including during beta testing and the testing and review process, and prior to launching a new product.

• Develop, implement, and routinely update a tailored, risk-based sanctions compliance program that includes sanctions list and geographic screening and other appropriate measures as determined by the company's unique risk profile.

• Utilize geolocation and IP address blocking controls and email-related restrictions for sanctioned jurisdictions. OFAC took enforcement action against BitGo, Inc. for failing to prevent users in sanctioned jurisdictions from accessing and using its platform, even though BitGo had the geolocation information in its possession.

• Collect customer identification information, including addresses (physical, digital wallet, IP). Utilize screening tools' fuzzy logic capability to account for common name variations and misspellings.

• Utilize transaction monitoring and investigation software.

• Create a keywords list of a sanctioned jurisdiction's cities and regions to be used when screening "Know Your Client" information.

• Review and update end-user agreements to include information about US sanctions requirements.

• Conduct retroactive batch screening of all users, including not only for direct customers, but also for individuals who may be otherwise involved in a virtual currency transaction. For example, OFAC recently reached a settlement agreement with US virtual currency payment service provider

BitPay, Inc. for processing virtual currency transactions between the company's customers and persons located in sanctioned jurisdictions. Although BitPay's sanctions compliance controls included screening its direct customers (merchants in the US and elsewhere), the company did not screen available information about the individuals who used its payment processing platform to buy products from those merchants.

Conclusion

OFAC's guidance puts those associated with the virtual currency industry on notice that they must consider sanctions risks and compliance in their virtual currency-related transactions. Attorneys in our National Security, Sanctions, and Export Controls and Data Privacy and Cybersecurity Practices stand ready to help you assess virtual currency risks and improve your internal risk-based compliance programs.

Contact Us

Rachel K. Alpert
ralpert@jenner.com | Download V-Card

Shoba Pillay
spillay@jenner.com | Download V-Card

Emily A. Merrifield
emerrifield@jenner.com | Download V-Card

Meet Our Team

Practice Leaders

Paul Feldberg
Co-Chair
pfeldberg@jenner.com
Download V-Card

Rachel K. Alpert
Co-Chair
ralpert@jenner.com
Download V-Card

AMB. David Pressman
Co-Chair
dpressman@jenner.com
Download V-Card