November 10, 2021

Skadden


If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys listed on the last page or call your regular Skadden contact.



One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Avenue, N.W.
Washington, D.C. 20005
202.371.7000

*This is the first of a series of articles in which we discuss recent efforts by U.S. regulators and other bodies to set expectations and standards with respect to cryptocurrencies and other virtual assets and the impact of these efforts on businesses engaged in virtual asset activities.*

## US Treasury Provides Detailed Guidance for the Virtual Currency Industry on Sanctions Compliance

On October 15, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issued detailed guidance to the virtual currency industry, putting virtual currency companies on notice of the ways OFAC expects them to comply with U.S. sanctions. It is OFAC's most comprehensive treatment to date of sanctions compliance considerations for virtual currency activities.

In its "Sanctions Compliance Guidance for the Virtual Currency Industry" (Guidance), OFAC directs startup businesses dealing with virtual currencies[1] to begin designing their compliance programs before operations commence. It also outlines how businesses in this space should screen customers and transactions for potential sanctions nexuses, including through the use of geolocation technology. OFAC also stresses the importance of independent testing and employee training that is tailored to the risks presented by a company's business.

The Guidance applies to all persons operating in the virtual currency space, including technology companies, exchangers, administrators, miners and wallet providers, as well as more traditional financial institutions that may have exposure to virtual currencies or their service providers. The document reflects the growing focus of various federal regulatory agencies on how to best mitigate financial crime and other related risks associated with these assets.

### I. Background to the Guidance

The Guidance builds on OFAC's May 2, 2019, "A Framework for Sanctions Commitments," (Compliance Framework) and articulates OFAC's expectations and its view of best practices for companies operating in the virtual currency industry. It comes against

[1] Virtual currency, as defined by OFAC in its frequently asked questions (FAQs), encompasses cryptocurrency as well as other "digital representation[s] of value that function[] as (i) a medium of exchange; (ii) a unit of account; and/or (iii) a store of value; and [are] neither issued nor guaranteed by any jurisdiction." FAQ 559.

a backdrop of increasing OFAC enforcement activity involving virtual currency businesses, including OFAC's first-ever designation of a virtual currency exchange under OFAC's sanctions authority on September 21, 2021.[2] The Guidance also coincided with a report issued by the Treasury Department's Financial Crimes Enforcement Network (FinCEN) outlining FinCEN's analysis of ransomware trends in Bank Secrecy Act reporting over the first six months of 2021.

Moreover, as we described in an October 26, 2021, client alert, the Treasury Department released the results of its broad review of OFAC's economic and financial sanctions on October 18, 2021, which noted that cybercriminals and other malicious actors often use evolving technologies, such as virtual currencies, in an effort to avoid the reach of U.S. sanctions. Taken together, these actions indicate virtual currency regulation and enforcement are likely to remain front-of-mind for the Treasury Department in the near term, including at OFAC and FinCEN.

## II. Sanctions Compliance Program Expectations and Best Practices

The Guidance reiterates the five essential components of a compliance program set forth in the Compliance Framework: (1) management commitment, (2) risk assessment, (3) internal controls, (4) testing and auditing, and (5) training. OFAC outlines how virtual currency companies should tailor their sanctions compliance programs to meet the unique risks posed by virtual currencies. OFAC considers sanctions compliance obligations to apply equally to both virtual currency transactions and those involving fiat currencies.

### Management Commitment and Sanctions Risk Assessments

The Guidance observes that members of the virtual currency industry often implement OFAC sanctions policies and procedures months, or even years, after commencing operations, which can expose such companies to a variety of potential sanctions risks. OFAC therefore recommends that virtual currency companies consider sanctions compliance during the technology and product testing and review processes so that sanctions compliance can be addressed prior to launch.

OFAC expects that a sanctions compliance program will be risk-based. A routine (or, if necessary, ongoing) risk assessment is therefore crucial in tailoring an appropriate program. An important part of that assessment is understanding who is accessing a virtual currency company's platform or services, and the Guidance notes that this may help members of the virtual currency industry identify the appropriate screening standards to set for each of their products and services.

### Internal Controls

OFAC recommends several best practices that virtual currency companies consider to strengthen their internal sanctions compliance controls.

- **Geolocation Tools.** Geolocation tools and IP address blocking controls are cited as crucial. Companies should be able to identify and prevent IP addresses from prohibited or otherwise unauthorized jurisdictions from accessing a company's website and services. The Guidance notes that OFAC has taken enforcement action against companies in the virtual currency industry that have engaged in prohibited activity that occurred, in part, due to a failure to use geolocation information in their possession.
- **Screen Relevant Data.** OFAC expects that companies will screen the customer and transactional data available to them against OFAC-administered sanctions lists, including the List of Specially Designated Nationals and Blocked Persons. A company's sanctions screening function should incorporate fuzzy logic, where relevant, and account for updates to customer information and sanctions lists, and changes in regulatory requirements.
- **Know-Your-Customer Procedures.** The Guidance recommends that virtual currency companies obtain information about their customers during onboarding and throughout the lifecycle of the customer relationship and use this information to conduct due diligence sufficient to mitigate the customer's potential sanctions-related risk. Higher-risk customers in the virtual currency space may warrant additional due diligence. Additional due diligence may include, for example, examining customer transactional history for connections to sanctioned jurisdictions or transactions with virtual currency addresses that have been linked to sanctioned actors.
- **Transaction Monitoring and Investigation.** Transaction monitoring and investigation software products are important tools to identify transactions involving virtual currency wallet addresses associated with sanctioned individuals or entities located in sanctioned jurisdictions. These tools should be used to review historical information relating to wallet addresses or other identifying information, the Guidance states, and may help companies better understand their exposure to sanctions risks and identify sanctions compliance program deficiencies.

OFAC does not require companies to use any particular compliance systems or software, but these tools can help support an effective sanctions compliance program, especially in the context of higher-risk customers that may require additional scrutiny.

[2] In designating the exchange, OFAC determined that over 40 percent of the exchange's transactions involved illicit activity and that the exchange had provided material support to criminal ransomware actors. OFAC made that designation concurrently with its issuance of an updated advisory relating to the potential sanctions risks associated with facilitating ransomware payments, which are often made using virtual currencies.

### Testing and Auditing and Training

OFAC notes that an independent testing or audit function is critical to assessing whether a sanctions compliance program is operating as intended and is commensurate to the risks presented by a virtual currency company's business. The Guidance also reiterates prior policy on the importance of providing sanctions compliance training that is tailored to the company's specific risk and business profiles to all employees (including compliance, management, and customer service personnel) on a periodic basis, and, at minimum, annually.

## III. Additional Interpretive Guidance

The Guidance and the updated frequently asked questions that accompanied it also provide interpretive advice to companies and financial institutions. The Guidance and OFAC's FAQ 646, for instance, clarify that a U.S. person that identifies virtual currency that should be blocked pursuant to U.S. sanctions is not obligated to convert the blocked virtual currency into traditional fiat currency (*e.g.*, U.S. dollars) prior to blocking the property, and is not required to hold the blocked property in an interest-bearing account. As with any blocked property, however, blocked virtual currency must be reported to OFAC within 10 business days and on an annual basis thereafter, so long as the virtual currency remains blocked.

OFAC has not said, however, how parties that host or maintain virtual currency wallets are supposed to reject incoming transfers on the blockchain. Rejection of these transactions remains a challenge for virtual currency companies in light of the instantaneous and irreversible nature of blockchain transfers.

## IV. Conclusion

As virtual currencies have grown in popularity and sophistication, they, and the companies that deal in them, have come under increasing scrutiny by federal regulators. The Guidance provides new detail about what OFAC expects virtual currency companies to do to prevent sanctions violations. In light of the Guidance, virtual currency companies, including fintechs and cryptocurrency exchanges, should reassess whether their compliance programs are adequate to address the unique risks presented by their business activities.

## Contacts

**Jamie L. Boucher**
Partner / Washington, D.C.
202.371.7369
jamie.boucher@skadden.com

**Eytan J. Fisch**
Partner / Washington, D.C.
202.371.7314
eytan.fisch@skadden.com

**Bao Nguyen**
Partner / Washington, D.C.
202.371.7160
bao.nguyen@skadden.com

**Greg Seidner**
Associate / Washington, D.C.
202.371.7014
greg.seidner@skadden.com

**Vartan Shadarevian**
Associate / Washington, D.C.
202.371.7363
vartan.shadarevian@skadden.com

**Javier A. Urbina**
Associate / Washington, D.C.
202.371.7376
javier.urbina@skadden.com