Updates
October 19, 2021

OFAC Releases New Detailed Guidance for the Digital Currency Industry

On October 15, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) released guidance on sanctions compliance for the digital currency industry, the agency's most detailed guidance to date on its expectations for participants in this rapidly growing industry.

OFAC's guidance arrives amidst increasing scrutiny of the industry by various federal regulators and just weeks after the agency issued an advisory on ransomware payments and took the unprecedented enforcement action of placing a cryptocurrency exchange, SUEX OTC, on OFAC's Specially Designated Nationals (SDN) list. The Department of the Treasury's press release highlights that the guidance is a continuation of the Biden administration's "whole-of-government" effort to combat ransomware. Given the technological and operational differences between digital currency companies and traditional financial institutions, the specificity and detail OFAC included in its guidance provides useful insight for participants in this evolving ecosystem.

In this update, we briefly summarize OFAC's guidance, highlighting practical implications for both digital currency companies and customers. OFAC's guidance defines the digital currency industry to include not just exchangers and administrators, but also wallet providers and, notably, technology companies and miners.

U.S. Economic Sanctions and Digital Currencies

The guidance begins with an instructive primer on the U.S. economic sanctions framework—including how it relates to digital currencies. OFAC provides (1) a distinction between virtual and digital currencies, (2) an overview of how to "block" digital currencies, and (3) an explanation of OFAC's strict liability regime.

Digital Currencies v. Virtual Currencies. OFAC defines virtual currencies as a subset of assets within the larger category of digital currencies. OFAC's guidance and newly updated FAQs, however, use the terms interchangeably. Thus, OFAC's compliance expectations appear to be largely the same regardless of whether digital currency industry participants are dealing with digital currencies or virtual currencies (as OFAC defines them).

Digital Currency "Blocking." OFAC regulations require that U.S. persons deny all parties access to digital currency that is required to be blocked. While OFAC requires that blocked fiat currency be placed into an interest-bearing account, OFAC clarifies in this guidance that companies have no obligation to convert blocked digital currency into a fiat currency and place the resulting fiat into an interest-bearing account.

Strict Liability. OFAC explains that sanctions violations are strict liability offenses—i.e., a U.S. person violates U.S. sanctions by engaging in a prohibited transaction, even if inadvertently. While this may seem intimidating, in practice OFAC has considerable discretion in determining the appropriate action to take in response to apparent U.S. sanctions violations. A key factor in its enforcement decisions will be whether the U.S. person has followed this guidance and OFAC's previously published "Framework for OFAC Compliance Commitments" (Framework) on which the guidance builds.

OFAC May 2019 Framework for OFAC Compliance Commitments

In May 2019, OFAC published its first guidance addressing essential steps for implementing an effective Sanctions Compliance Program (SCP). The OFAC 2019 guidance may be found here and our May 2019 update regarding the Framework may be found here. In its 2019 guidance, OFAC stated that each SCP program should incorporate at least five essential components: (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training.

In its current guidance, OFAC expands on these five pillars by specifying best practices for implementing a SCP program for the digital currency industry. OFAC's suggestions, which ultimately tie back to a risk-based approach towards sanctions compliance, are notable for their specificity.

Management Commitment. As with traditional financial services companies, it is the responsibility of senior management to "ensure sanctions compliance efforts receive adequate resources and are fully integrated into the company's daily operations." OFAC flags this as important because of the perception that participants in the digital currency industry have often delayed implementation of an SCP.

Risk Assessment. Similar to its discussion of management commitment, OFAC's expectations for risk assessments are not markedly different for the digital currency industry than for other industries or markets. OFAC recommends that companies conduct a complete review of their potential exposure to transactions or parties subject to U.S. economic sanctions and try to minimize any such risk, through identification and screening of customers and by implementing enhanced safeguards for high-risk customers and/or counterparties.

For the digital currency industry, the key will be to tailor the risk assessment process to each company's particular business model and customer base. This may prove challenging in light of fundamental aspects of the digital currency ecosystem—most notably that it is not always possible to have full transparency into the counterparties of a transaction. For this reason, among others, OFAC notes that the digital currency industry poses higher-than-standard risks for potential sanctions evasion. In approaching risk assessment and the design of appropriate SCPs, participants in the digital currency industry must account for this perception and recognize the likely high standards the agency will have for their SCPs. In particular, notwithstanding the lack of further guidance on the non-transparent counterparties issue, OFAC will expect companies to implement an SCP that addresses the issue in the context of their operations.

Internal Controls. An effective risk assessment requires that a company implement well-designed and effective internal controls to conduct due diligence and monitor customers, business partners, and transactions. OFAC emphasizes in this guidance that internal controls should be risk-based and tailored to a company's activities.[1] In particular, the agency explains that industry participants should take the following actions:

- *Screen available data.* OFAC guidance highlights an expectation that industry participants should incorporate all data collected into its SCP. This data can include email addresses, invoices, and other transaction information.
- *Incorporate geolocation tools, IP address blocking controls, and sanctions screening.* OFAC's guidance states that "virtual currency companies with strong SCPs should be able to use geolocation tools to identify and prevent IP addresses that originate in sanctioned jurisdictions from accessing a company's website and services for activity that is prohibited by OFAC's regulations, and not authorized or exempt." This guidance sets an agency expectation that industry participants take affirmative steps to reasonably prevent IP addresses from sanctioned locations from accessing their platform. Like the discussion of strict liability above, this guidance should be more helpful than intimidating: In the event of a misstep, where a company has documented its efforts to implement this guidance and meet OFAC's expectations, OFAC

may take this into consideration when evaluating a company's potential violation along with the overall strength of the company's SCP.
- *Use transaction monitoring and investigation software.* OFAC recommends adopting software solutions to identify transactions involving digital currency addresses associated with sanctioned individuals and entities listed on the OFAC sanctions list or located in sanctioned jurisdictions. Helpfully, OFAC is now including digital currency identifiers in its sanctions listings wherever available. Companies should look beyond basic screening of participants for potential sanctioned party associations, including screening for addresses not listed on OFAC's SDN list but which nonetheless may present sanctions exposure because the addresses are associated with the same wallet cluster as a listed address. For digital currency companies, this can be addressed by regularly screening transactions on a blockchain analytics tool like Chainalysis' KYT and reporting to OFAC as necessary.

Testing and Audits. OFAC requires companies to properly test and audit the effectiveness of their SCP. A company may not realize that its screening and other critical compliance systems are not functioning properly until it is too late. Participants in the digital currency industry should build into their SCPs a regular auditing and testing schedule to analyze the effectiveness of their SCPs in practice.

Training. OFAC notes that training should be provided to all appropriate employees on a periodic basis, at minimum, annually. As with all aspects of OFAC's requirements, the training should be tailored to reflect the employee's activities, and the company's business structure and risk profile. OFAC recommends that trainings account for the frequent changes to sanctions programs and to the new technologies employed in the digital currency space.

Takeaways and Unresolved Issues

The most significant takeaways from the guidance are

- OFAC expects all companies involved in the digital currency industry to adopt an SCP and has begun to develop specific standards for evaluating the effectiveness of such programs; and
- OFAC has discretion in determining its enforcement response to a sanctions violation and likely will favor a company that has a thoughtful and rigorous SCP.

While the guidance provides more clarity for the digital currency industry, unaddressed issues nevertheless remain, which include the following:

- *Rejecting Transactions.* While OFAC states that digital currency industry participants are to reject certain transactions, its guidance does not wrestle with the reality that, to our knowledge, there is no practical way for exchanges to reject incoming deposits from prohibited counterparties. In addition, in some cases, there may be no practical means of identifying whether outbound transactions from exchanges or wallet products are directed to prohibited counterparties. Further clarity from OFAC regarding how to handle such situations would be helpful.
- *Indirect Exposure.* OFAC applies liability for indirect exposure to a sanctioned party. This is particularly perilous for the digital currency industry, where there is often no way to know where the asset will eventually rest after the first transfer of a digital currency from the exchange to an external wallet address. While OFAC did not address this point, it bears noting that OFAC's enforcement guidance places significant focus on the strength of a company's compliance program and their efforts to evaluate available data to prevent sanctions violations. This may mitigate the risks of enforcement for digital currency companies with robust compliance mechanisms even in circumstances where an indirect transaction with a sanctioned party may evade their controls.

- *Counterparties.* The digital currency industry is at a disadvantage because it cannot always identify counterparties to a transaction. However, there are existing tools that can assist a company in identifying high-risk wallet addresses and, accordingly, help the company mitigate the risk that it transfers digital currency to an address associated with a sanction party. Digital currency industry participants should incorporate services like these into their compliance program.
- *Decentralized Autonomous Organizations (DAOs).* While many digital currency companies will be able to build out a compliance program that satisfies OFAC under the framework provided in this guidance, aspects of the guidance need more clarity as to how they may apply to DAOs. For example, a DAO may not have an identifiable senior management to set a tone regarding the importance of OFAC sanctions, or to enforce OFAC-related controls. Further, it is unclear who in a DAO should be trained to ensure that sanctions laws are not being violated.

Please contact experienced economic sanctions counsel with questions about this guidance and how it might apply to your business.

Endnote

[1] In designing and deploying sanctions compliance controls, companies also need to properly document their efforts. For example, industry participants should be prepared to present diligence files reflecting their reasonable reliance on service provider partners responsible for IP address screening. Companies should also periodically test their data collection procedures to account for avoidable human error. OFAC notes, for example, that a company should ensure that it accounts for name variations and misspellings of names and locations to the best of the company's ability. The process and procedures involved in such efforts should be properly documented.

Authors

Richard W. Oehler

Partner
ROehler@perkinscoie.com 206.359.8419

Jamie A. Schafer

Partner
JSchafer@perkinscoie.com 202.661.5863

Steven D. Merriman

Partner
SMerriman@perkinscoie.com 206.359.3495

Explore more in

White Collar & Investigations Fintech

Related insights

Update

'Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers

Update

Employers and Immigration Under Trump: What You Need To Know