OFAC Puts Virtual Currency Industry on Notice, Highlights Best Practices for Digital Commerce

October 27, 2021

On October 15, 2021, the Office of Foreign Assets Control (OFAC) issued an advisory providing sanctions compliance guidance for the virtual currency industry (Guidance). The Guidance follows a series of recent enforcement actions targeting the industry and the designation of a cryptocurrency exchange for facilitating ransomware payments. These developments highlight OFAC's continued focus on this sector and virtual currency, which is seen as a potential tool to evade U.S. sanctions and diminish the efficacy of U.S. sanctions policy.

The Guidance provides additional insight into OFAC's expectations with respect to identifying sanctioned parties online, which is helpful for any company that provides services to customers over the internet, even if not directly dealing with virtual currencies.

Level setting

As an initial matter, OFAC cautions that its rules apply to virtual currency transactions to the same extent that they apply to transactions involving fiat currencies. For example, U.S. persons remain subject to the prohibitions on dealing with sanctioned jurisdictions (Cuba, Iran, North Korea, Syria, or Crimea) and sanctioned parties when they are conducting transactions denominated in virtual currencies or engaging in related services. And non-U.S. persons can similarly face penalties for violating U.S. sanctions if their conduct involves the United States, U.S. persons, or goods or services that originate from the United States.

As with fiat currency, OFAC's Guidance confirms that participants in the virtual currency space must "block" virtual currency by denying all parties access to the asset and report the blocked property to OFAC within 10 business days. However, there is no requirement to convert the virtual currency into fiat currency or to hold the virtual currency in an interest-bearing account, unlike other blocked funds.

Best Practices for the Virtual Currency Industry

The Guidance strongly recommends that industry members adopt a risk-based approach to sanctions compliance based on OFAC's "Framework for OFAC Compliance Commitments." OFAC notes that traditional financial institutions and other companies with exposure to virtual currencies or related service providers should adopt appropriate controls to address sanctions risks. These include:

Management Commitment – Many members of the fast-growing virtual currency industry may be slow to develop and implement sanctions compliance programs, which can risk exposure to sanctions violations. OFAC counsels early managerial commitment to the development and

implementation of compliance programs. Building these processes in early can prevent costly violations later on.

Risk Assessment – The Guidance recommends that companies conduct routine risk assessments to identify potential sanctions issues before providing services or products to customers. The risk assessment should be tailored to what and where products or services are offered, account for customers, reflect the company's supply chain, and also evaluate counterparty and partner risk, including whether those parties have adequate compliance procedures. The results of that assessment should feed into the development of an effective sanctions compliance policy. Outside advisors can help craft risk assessments that highlight key risks for virtual currency companies.

Internal Controls – The Guidance document contains a number of recommendations related to internal controls and processes that should be considered in designing a sanctions compliance program for virtual currencies and digital payments. As noted above, many of these recommendations apply to any company that provides digital services over the internet and reflect lessons learned from recent enforcement actions targeting online commerce. These tools include:

- Geolocation and IP Address Blocking – As in several recent enforcement actions (including those involving Payoneer, BitGo, and Amazon), the Guidance makes clear that OFAC expects companies to consider IP address geolocation data to identify customers that may be in or ordinarily reside in sanctioned jurisdictions and to adopt blocking controls that deny access to IP addresses associated with sanctioned jurisdictions. OFAC notes that analytics tools can play an important role in identifying the likely location of customers by addressing IP address geolocation misattribution caused by the use of anonymization services like Virtual Private Networks (VPNs). Other information, such as an address from a customer or counterparty, an email address top-level domain (e.g., user@domain.ir or user@domain.gov.ir), or transactional details, like an invoice, can also be relevant for a company's sanctions controls, even if that information was initially obtained for a non-compliance purpose.

- Know Your Customer (KYC) Procedures – Conducting due diligence at onboarding, during periodic reviews, and when processing transactions helps to reduce potential sanctions-related risks. For individuals, this means screening customers' names, dates of birth, physical and email addresses, nationality, IP addresses associated with transactions and logins, bank information, and government-issued or other documentation against sanctions lists (like the SDN List) and for any "red flags." For entities, this can also include type of business, ownership information, physical and email address, and where the entity does business. A keyword list of sanctioned jurisdiction cities and regions can also be an important part of a KYC screening.

- Transaction Monitoring and Investigation – OFAC's Guidance endorses the use of software to monitor and investigate transactions involving sanctioned individuals and entities or persons located in sanctioned jurisdictions based on identifying information associated with transaction data. As of 2018, OFAC began to include virtual currency addresses in the "ID #" field for persons listed on the SDN List. Companies should calibrate software to identify and block transactions associated with those virtual currency addresses, in addition to those otherwise associated with SDNs or persons located in sanctioned jurisdictions.

- Implementing Remedial Measures – Should a virtual currency company identify an apparent sanctions violation, that company should take immediate and effective remedial actions, which OFAC may consider as a mitigating factor in a potential enforcement action.

- Monitoring Transactions and Users for "Red Flags" – OFAC's Guidance notes that there are

several “red flags” that may indicate a transaction’s or user’s connection to sanctions, including providing inaccurate or incomplete KYC information at onboarding; attempting to access a virtual currency exchange from an IP address or VPN connected to a sanctioned jurisdiction; failing or refusing to provide updated KYC information or to provide requested additional transaction information; and, attempting to transact with a virtual currency address associated with a blocked person or a sanctioned jurisdiction.

Testing and Auditing – OFAC’s Guidance advises that companies operating in the virtual currency industry test and audit their sanctions compliance programs to ensure they are operating as intended, and highlights a few best practices, such as:

- Ensuring sanctions and KYC screening tools effectively flag transactions and customers related to SDNs or sanctioned jurisdictions;
- Confirming IP address software properly prevents sanctioned jurisdiction access; and
- Reviewing procedures for investigating and, if applicable, blocking and reporting to OFAC flagged transactions identified through the screening process.

Training – The Guidance stresses the importance of conducting, on at least an annual basis, mandatory training that is informed by the profile of the company and tailored to the responsibilities and functions of all relevant employees. Especially in the virtual currency industry, sanctions training should take into account frequent developments and updates regarding both the governing sanctions programs and underlying technologies in the virtual currency space.

Final Considerations

The publication of the Guidance underscores the growing importance of implementing effective sanctions compliance programs tailored to the risks presented by virtual currencies given increased OFAC and U.S. government focus on the sector. The Guidance is another signal that OFAC will be ramping up enforcement efforts to address illicit activities in which cryptocurrencies and digital payment services play a large role.