Sanctions Compliance Guidance for the Virtual Currency Industry and updated frequently asked questions

28 October 2021

In response to the rapid growth of virtual currencies, the Treasury Department's Office of Foreign Assets Control ("OFAC") recently published Sanctions Compliance Guidance for the Virtual Currency Industry ("Guidance").

The Guidance clarifies the applicability of OFAC sanctions to virtual currencies and outlines a number of steps that financial institutions, technology companies, exchanges, administrators, miners, wallet providers, and other firms can take to minimize the risk of violating OFAC sanctions.

OFAC Sanctions Apply to Virtual Currencies

The Guidance makes it clear that OFAC sanctions apply to transactions involving virtual currencies, and that members of the virtual currency industry are responsible for ensuring that they do not engage, directly or indirectly, in transactions prohibited by OFAC sanctions. This includes financial dealings of any kind with blocked persons or property, and transactions that cause a U.S. person to violate sanctions.

Given the broad jurisdictional reach of OFAC sanctions, any virtual currency business operating in the United States, organized under the laws of the United States (including foreign branches of U.S. entities), or engaging in transactions involving U.S. persons must be aware of OFAC sanctions requirements. It is important to note that OFAC may impose civil monetary penalties even if a violator has no knowledge or reason to know that it is engaging in prohibited conduct.

OFAC Requirements and Procedures

Although not every OFAC sanctions program is the same, there are certain basic requirements and procedures that apply uniformly. Most importantly, once an entity subject to OFAC regulations determines that it holds blocked property, the entity must deny all parties access to that property and file a report to OFAC within 10 business days. There are also additional reporting and recordkeeping requirements, as well as license procedures.

Best Practices for the Virtual Currency Industry

The Guidance encourages all companies in the virtual currency industry to develop, implement, and routinely update a risk-based compliance program. According to OFAC, companies should tailor compliance programs to fit their unique risk profile, which will depend on factors such as the company's business, size, sophistication, products, services, customers, and counterparties, as well as the geographic locations in which the company operates.

The Guidance highlights five essential components of any successful sanctions compliance program:

- management commitment
- risk assessment
- internal controls
- testing and auditing
- training

Management Commitment

OFAC notes that it often takes companies in the virtual currency industry months, or even years, to implement a sanctions compliance program. This leaves virtual currency companies exposed to a variety of potential sanctions risks. Accordingly, the Guidance encourages senior management to think about sanctions compliance during the testing and review process of their operations, and to build compliance procedures into new products and services. OFAC also recommends that senior management review and endorse sanctions compliance policies, provide adequate resources to enforce these policies, delegate sufficient autonomy and authority to the compliance unit, and appoint a dedicated sanctions compliance officer.

Risk Assessment

In addition to conducting a risk assessment prior to developing a sanctions compliance policy, OFAC urges companies to conduct ongoing reviews of their dealings in foreign jurisdictions and with foreign persons. This may be the only way for companies to identify potential weak spots in their internal controls. A settlement earlier

this year between OFAC and a U.S. virtual currency payment service provider underscored the importance of diagnosing and quickly addressing potential sanctions risks. Although the company screened its direct customers, it failed to screen individuals who used its platform to buy products from those customers. As a result, the company inadvertently processed virtual currency transactions between some of its customers and persons located in sanctioned jurisdictions.

Internal Controls

One of the most important features of an effective sanctions compliance program is a robust system to identify and address red flags. This requires a set of internal controls, which generally include tools to screen customers, monitor transactions, and investigate potential sanctions violations. The manner in which virtual currency transactions take place can make this a significant challenge.

For example, OFAC has noticed that users in sanctioned jurisdictions frequently try to access virtual currency products and services. In 2020, OFAC entered into a settlement with a US company that offers digital asset custody, trading, and financing services for allowing this to happen. Even though the company collected its users' IP addresses, it did not use this information to screen for and block suspicious transactions. As a result, the company processed transactions on behalf of individuals in sanctioned jurisdictions.

The Guidance lays out a set of best practices for companies looking to strengthen their internal controls. These include implementing geolocation tools, IP address controls, know your customer (KYC) procedures, and transaction monitoring and investigation software. When used in combination, these tools can help screen customer information against OFAC sanctions lists, screen transactions to identify addresses, including physical, digital wallet, and IP addresses, and account for common name variations and misspellings with fuzzy logic capabilities.

When a company's internal controls identify an apparent sanctions violation, taking immediate and effective remedial action may be a mitigating factor in any potential sanctions enforcement action. OFAC lists a number of remedial measures that virtual currency companies have taken in the past, including:

- implementing IP address blocking and email-related restrictions on sanctioned jurisdictions
- reviewing and updating end-user agreements to include information about sanctions requirements
- conducting retroactive batch screening of all users
- hiring additional compliance staff

Testing and Auditing

Once a sanctions compliance program is in place, OFAC emphasizes the need for companies in the virtual currency industry to independently test and audit their sanctions policies and procedures. This is particularly important for technology firms whose risk profiles are continuously changing. OFAC recommends that the testing and auditing function focus primarily on sanctions list screening, keyword screening, IP blocking, and investigation and reporting.

Training

Lastly, the Guidance underscores the importance of sanctions-specific training. OFAC recommends that virtual currency companies provide training to all compliance, management, and customer service personnel. This training should account for frequent changes to OFAC sanctions programs, and address the risks that new and emerging software and technology may pose.