Foreign Investment & Trade Alert

Weil

October 25, 2021

OFAC Issues Sanctions Compliance Guidelines for Virtual Currency Industry

By Shawn Cooley, Timothy Welch and Glenda Bleiberg

On October 15, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) published a brochure on "Sanctions Compliance Guidance for the Virtual Currency Industry," aimed at providing compliance guidance for this rapidly growing sector. In addition, OFAC also updated two of its related Frequently Asked Questions (FAQs). In essence, OFAC is trying to increase awareness of its efforts to prevent U.S. persons from dealing with sanctioned persons or jurisdictions, or engaging in unauthorized transactions using virtual currencies. According to FAQ No. 559, virtual currency is defined as "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." Once a U.S. person determines that they hold virtual currency that is required to be blocked pursuant to OFAC's regulations, FAQ No. 646 clarifies that the U.S. person must deny all parties access to that virtual currency, ensure that they comply with OFAC regulations related to the holding and reporting of blocked assets and implement controls that align with a risk-based approach.

Although the sanctions that OFAC administers are strict liability regimes, OFAC generally takes into consideration the totality of facts and circumstances when determining an appropriate enforcement response. OFAC strongly encourages a risk-based approach to sanctions compliance that is specially tailored to the virtual currency world. Such approaches should be developed, implemented and regularly updated by all companies in the industry, including "technology companies, exchangers, administrators, miners and wallet providers," and more traditional financial institutions with potential exposure to virtual currencies or their service providers. The risk-based approach should take into consideration a variety of factors, including the type of virtual currency business, its size and sophistication, the nature of the products and services it offers, its customers and counterparties and the geographic locations served.

In order to avoid violating U.S. sanctions laws in connection with virtual currency, OFAC recommends implementing a sanctions compliance program with five essential components, which should be developed prior to providing products or services to customers, namely:

i. **Management Commitment:** Considered critical by OFAC, management should be committed to: a) reviewing and endorsing sanctions compliance policies and procedures; b) making sure to commit adequate resources, including personnel, expertise, information, technology and other resources to support the compliance function; c) providing the compliance unit with enough autonomy and authority; and d) appointing a sanctions compliance officer with the necessary technical expertise.

ii. **Risk Assessment:** The sanctions compliance risk assessment should entail an overall review of the company in order to assess touchpoints with foreign jurisdictions or persons and mitigate the risk of any exposure to sanctions. A tailored risk assessment should consider a company's customer or client base, products, services, supply chain, counterparties, transactions and geographic locations and may entail the assessment of the compliance procedures of counterparties and business partners.

iii. **Internal Controls:** In order to identify and prevent sanctioned individuals or IP addresses located in sanctioned jurisdictions from using a company's website/platform for illegal activities, OFAC specifically recommends the use of "geolocation tools" and IP address blocking controls. Further, analytical tools can be used to identify IP misattribution that may result from the use of virtual private networks (VPNs). OFAC stresses the need to include, as part of the sanctions compliance program, the review of all available information that a virtual currency company may collect on particular transactions in sanctioned jurisdictions, either coming from customers or counterparties, e-mail addresses, invoices or from other sources (irrespective of why it was collected). Internal controls should also include:

- The implementation of Know Your Customers (KYC) procedures: As part of the information regularly gathered from onboarding and during the life cycle of the costumer relationship, companies should keep IP addresses associated with transactions and logins, bank information, relevant government documents and information on residency/where the entity does business. Additional due diligence may be required for higher risk customers. Information gathered in the context of compliance with anti-money laundering laws may also be useful to assess and mitigate risk.
- Transaction monitoring and investigation: Transaction monitoring and investigation software can help identify transactions involving virtual currency addresses or other identifying information of sanctioned individual or entities, and to block transactions with such individuals or entities. The tool may also be used to review historical information linked to such addresses and information in order to assess risk exposure and flag potential weaknesses of the compliance program. OFAC has included virtual currency addresses connected to sanctioned individuals/entities in the Specially Designated Nationals And Blocked Persons (SDNs) List. The listed virtual currency addresses may help identify other virtual currency addresses that may be associated with SDNs. (*e.g.*, virtual currency addresses sharing a wallet, which may indicate that the non-listed address is also linked to a blocked person). Virtual currency companies may consider conducting a historical look back at transactions following OFAC's list of a virtual currency address in order to identify other connections to the listed address.
- Sanctions screening: Suggested to be an essential part of the internal controls, screening may include geolocation tools and more. Among the best practices related to screening are the following: screening at onboarding; screening transactions to flag virtual addresses, including wallets and IP addresses and other relevant information regarding sanctioned persons of jurisdictions; and continuing sanctions screening and risk-based re-screening to cover updates in OFAC's lists and other regulatory changes.
- Implementation of remedial measures: OFAC encourages virtual currency companies to implement remedial measures immediately once an issue/weakness with the compliance internal controls has been identified (including a potential sanctions violation). This may be considered a mitigating factor in an enforcement proceeding. Among the examples of remedial measures provided by OFAC are: employing IP address blocking and e-mail restrictions for sanctioned jurisdictions; using a key word list of sanctioned jurisdictions that includes cities and regions while conducting KYC screening; implementing retroactive batch screening of all users; hiring additional compliance employees and a dedicated chief compliance officer; and instituting OFAC compliance training for employees.

- Red flags: OFAC also recommends checking transactions and users for red flags that may indicate a sanctions nexus. Example of red flags include the submission of inaccurate or incomplete customer identification or KYC information when trying to open an account; attempting to access a virtual currency exchange from an IP address or VPN linked to a sanctioned jurisdiction; refusal to provide updated customer identification, KYC information, or additional transaction information; attempting to transact with a virtual currency address linked to a blocked person or sanctioned jurisdiction; and red flags suggesting anti-money laundering violations or other illegal activity.

iv. **Testing and Auditing:** In order to make sure that the compliance program is working effectively, companies should include comprehensive and independent testing or audits that would flag any issues with the program's performance or any need for updating due to changes in the risk assessment or sanctions framework. Virtual currency companies should ensure that their internal controls are working effectively in identifying transactions that need further review; flagging sanctioned jurisdictions and blocking users in sanctioned jurisdictions from accessing products or services from the company; and enabling the reporting to OFAC of blocked property and rejected transactions. The use of external and internal audits of the compliance program depends on the size or sophistication of a company.

v. **Training:** Periodic sanctions training, including job-specific knowledge and skills, should be provided to all relevant employees, and the training should take into account updates to sanctions programs as well as the new and emerging technologies in the virtual currency industry. The scope of the sanctions training depends on the size, sophistication and risk exposure of the company. At a minimum, training should be provided once a year and employees should be held responsible for completing the required training.

Key Takeaways:

OFAC's guidance and updated FAQs are in response to a dramatic rise in the use of virtual currencies and their potential for causing or facilitating illegal activities, including sanctions violations. Noncompliance with sanctions can result in significant criminal and civil penalties, as well as commercial and reputational damage. OFAC's guidance underscores for virtual currency companies the importance of instituting and maintaining robust sanctions policies and practices, both to promote compliance and as a mitigating factor in the event of noncompliance. This guidance also should be considered in conjunction with OFAC's Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments issued on September 21, 2021, in which it strongly opposes ransom payments and provides guidance on the sanctions risks associated with making ransomware payments, which tend to be in virtual currencies.

* * *

If you have questions concerning the contents of this alert, or would like more information, please speak to your regular contact at Weil or to the authors:

Authors

Glenda Bleiberg (D.C.)	View Bio	glenda.bleiberg@weil.com	+1 202 682 7016
Shawn Cooley (D.C.)	View Bio	shawn.cooley@weil.com	+1 202 682 7103
Timothy Welch (D.C.)	View Bio	timothy.welch@weil.com	+1 202 682 7132