Cooley

OFAC Issues Sanctions Compliance Guidance for Virtual Currency Industry

October 29, 2021

The US Department of the Treasury's Office of Foreign Assets Control (OFAC) recently issued **Sanctions Compliance Guidance for the Virtual Currency Industry**. The guidance **published on October 15, 2021**, outlines OFAC's expectations for virtual currency companies and other industry participants. It also provides a summary of OFAC resources and actions addressing virtual currency, including **previously issued answers to frequently asked questions (FAQs)**.[1]

In emphasizing the importance of implementing a tailored, risk-based sanctions compliance program, OFAC states that new and emerging companies (e.g., technology companies, exchangers, administrators, miners and wallet providers) sometimes do not implement sanctions policies and procedures until "months, or even years, after commencing operations." The guidance notes that OFAC sanctions compliance obligations are the same for all industries and that OFAC regulations apply equally to transactions involving virtual or fiat currency.

OFAC's recommended best practices

The OFAC guidance outlines certain sanctions compliance best practices specific to virtual currency companies and other industry participants. For example, OFAC recommends that virtual currency companies implement specific internal controls designed to identify and interdict virtual currency transactions that are prohibited by US sanctions. We've highlighted some of these internal controls below.

Using geolocation tools

According to OFAC, a strong sanctions compliance program includes the use of geolocation tools to identify and block users with IP addresses associated with jurisdictions that are subject to comprehensive sanctions (currently, Cuba, Iran, North Korea, Syria and the Crimea region of Ukraine) from accessing a company's platform or services in violation of US sanctions. In addition, OFAC suggests that certain geolocation tools could be used to identify IP misattribution, such as by screening against "known virtual private network (VPN) IP addresses" and identifying "improbable logins" (e.g., "the same user logging in with an IP address in the United States, and then shortly after with an IP address in Japan"). The guidance further notes that virtual currency companies should consider using all available information, such as information in email addresses or other transactional information, to identify users potentially in sanctioned jurisdictions.

Monitoring and investigating transactions

As another component of a strong compliance program, OFAC recommends that virtual currency companies monitor transactions and users for "red flags" or sanctions risk indicators, including information suggesting that a transaction or user is located in a sanctioned jurisdiction or identified on a sanctions list. Since 2018, OFAC has identified certain virtual currency addresses associated with blocked persons on the **Specially Designated Nationals and Blocked Persons (SDN) List**. OFAC notes that virtual currency industry participants should consider implementing tools and processes to block transactions involving such

addresses and other SDNs. The agency also suggests that virtual currency companies could use the listed virtual currency addresses to identify other virtual currency addresses that may be associated with blocked persons (e.g., "virtual currency addresses that share a wallet with a listed virtual currency address").

In addition, the guidance suggests that virtual currency companies should obtain sufficient know-your-customer (KYC) information from users to mitigate potential sanctions risks. However, we note many virtual currency companies do not collect or otherwise have access to KYC information (e.g., full names and addresses), particularly if they are not money services businesses subject to heightened KYC requirements under the Bank Secrecy Act. In these situations, where a virtual currency company's apparent violations can be attributed to a decision not to collect KYC information, OFAC is unlikely to show leniency.

Outlook

The release of the guidance, along with other recent actions by OFAC, the Treasury Department's Financial Crimes Enforcement Network (FinCEN) and the US Department of Justice, signal that the US government is increasingly focused on addressing sanctions and other risks posed by the virtual currency industry. Last month, **OFAC added a virtual currency exchange to the SDN List** for the first time for facilitating financial transactions involving illicit proceeds from ransomware actors. Before that, in **December 2020** and **February 2021**, OFAC entered into settlement agreements with two virtual currency companies for apparent sanctions violations involving the failure to monitor and block IP addresses associated with embargoed jurisdictions. Further, contemporaneous with the publication of OFAC's guidance on October 15, 2021, **FinCEN published an analysis of ransomware trends** in Bank Secrecy Act reporting filed in the first half of 2021, highlighting the use of virtual currency in ransomware attacks. Finally, this month, **the DOJ announced the creation of a National Cryptocurrency Enforcement Team** to investigate and prosecute criminal misuse of virtual currency.

The guidance represents OFAC's efforts to provide greater clarity regarding the applicability of US sanctions laws to the virtual currency industry. When evaluating a company's sanctions compliance program in an enforcement context, OFAC will likely look to the best practices outlined in the guidance. As we expect the virtual currency industry to continue to be an enforcement priority for OFAC, industry participants should consider the guidance in designing and implementing sanctions compliance policies and procedures specific to their particular risk profiles.

Notes

1. OFAC FAQ 559 (defining the terms "digital currency," "digital currency wallets," "digital currency addresses," and "virtual currency") and FAQ 646 (clarifying how to block virtual currency under OFAC's regulations) were updated on October 15, 2021.

Key Contacts

Adam Fleisher Washington, DC	afleisher@cooley.com +1 202 776 2027
Kevin King Washington, DC	kking@cooley.com +1 202 842 7823
Sarah Oliai Washington, DC	soliai@cooley.com +1 202 728 7149
Obrea Poindexter Washington, DC	opoindexter@cooley.com +1 202 776 2997
Rebecca Ross Washington, DC	rross@cooley.com +1 202 728 7150
Sean Ruff Washington, DC	sruff@cooley.com +1 202 776 2999
Karen Tsai Washington, DC	ktsai@cooley.com +1 202 842 7857