

OFAC publishes sanctions compliance guidance for the virtual currency industry

October 20, 2021 | Client Update | 5-minute read

A new OFAC guidance document sets out U.S. sanctions compliance requirements for the virtual currency industry and highlights OFAC's view of compliance best practices for that industry. The guidance presents an opportunity for industry participants to assess how their compliance practices measure up to OFAC's expectations.

A new guidance document from the U.S. Treasury Department's Office of Foreign Assets Control (OFAC), "[Sanctions Compliance Guidance for the Virtual Currency Industry](#)" (the Virtual Currency Guidance), summarizes sanctions compliance requirements for the virtual currency¹ industry and sets out OFAC's view of compliance best practices in that industry. Like other [industry brochures](#) published by OFAC, the Virtual Currency Guidance does not break new ground, but it provides a consolidated and user-friendly compilation of recent OFAC actions and resources. It provides a summary overview of the economic sanctions programs administered by OFAC, recordkeeping and reporting obligations, licensing and enforcement processes, OFAC's expectations regarding sanctions compliance programs as described in prior OFAC [guidance](#),² and links to relevant OFAC responses to Frequently Asked Questions and other content on OFAC's website.

Perhaps the most important takeaway from OFAC's publication of the Virtual Currency Guidance is that it signals the extent to which the virtual currency industry is likely to be a significant priority for OFAC (as it is for other agencies) in terms of both compliance outreach and enforcement going forward. This has also been reflected in recent enforcement cases, as well as OFAC's recent imposition of [sanctions](#) on a Russian virtual currency exchange that facilitated ransomware payments. Industry participants may wish to consider using the publication of the guidance as an opportunity to assess whether their sanctions compliance practices are consistent with OFAC's expectations and view of best practices as expressed in the guidance.

In particular, the Virtual Currency Guidance provides some useful insight into OFAC's view of compliance best practices specific to the virtual currency industry, including the following:

- **Sanctions compliance requirements need to be incorporated into business plans and product design from day one.** OFAC notes that it has "observed that members of the virtual currency industry implement OFAC sanctions policies and procedures months, or even years, after commencing operations, and that "[d]elaying development and implementation of a sanctions compliance program can expose virtual currency companies to a wide variety of potential sanctions risks." Accordingly, "OFAC encourages members of the virtual currency industry to evaluate their exposure to OFAC sanctions and take steps to minimize their risks—including through development of an appropriate sanctions compliance program—*prior to providing services or products to customers.*" (emphasis added). Consistent with its prior guidance on compliance programs, OFAC emphasizes the importance of formal compliance policies backed by sufficient resources and senior management commitment.
- **Geolocation tools and IP location blocking controls are key elements of a strong sanctions compliance program for virtual currency companies.** OFAC notes that without such controls, "virtual currency companies may fail to prevent persons who are located in comprehensively sanctioned jurisdictions from accessing their platforms or services to engage in prohibited activity." In addition to using such controls to block access from sanctioned jurisdictions, OFAC recommends the use of analytic tools to detect IP misattribution, which may indicate an attempt to

evade sanctions controls.

- **Virtual currency companies are expected to have robust “know your customer” procedures.** While many companies will be subject to formal AML requirements in any event, OFAC makes clear that it also expects best practices to include address and identity verification, suggesting that information gathered for onboarding and ongoing transaction monitoring may include name, date of birth, physical and email address, nationality, IP addresses associated with transactions and logins, bank information, and government identification and residency documents.
- **Companies will be held accountable if they have, but do not make use of, information relevant to sanctions compliance and violations occur as a result.** OFAC notes two recent enforcement cases in which virtual currency companies received, but did not screen, information indicating that customers or other parties to transactions were located in sanctioned jurisdictions. In the [first case](#), OFAC entered into a settlement agreement with a U.S. virtual currency payment service provider for processing virtual currency transactions between the company’s customers and persons located in sanctioned jurisdictions. While the company’s sanctions compliance controls included screening its direct customers, the company did not screen available information about the individuals who used its payment processing platform to buy products from those merchants, which indicated that those individuals were located in sanctioned jurisdictions. The [second case](#) involved a company’s failure to prevent use of its non-custodial secure digital wallet management service by individuals with IP addresses located in sanctioned jurisdictions. While the company collected IP address information for account security purposes, it did not apply sanctions-related controls to this information.
- **Virtual currency Addresses on the SDN List have uses beyond sanctions screening.** Beginning in 2018, OFAC started including virtual currency addresses as part of the identifying information for certain individuals or entities named on the List of Specially Designated Nationals and Blocked Persons (SDN List). OFAC expects companies operating in the virtual currency industry to employ tools sufficient to identify and block transactions associated with those virtual currency addresses included on the SDN List. Additionally, OFAC notes that inclusion of such addresses on the SDN List can assist the industry in identifying other virtual currency addresses that may be associated with blocked persons or otherwise pose sanctions risk, even if those other addresses are not explicitly listed on the SDN List.³ OFAC notes the value of blockchain analytics tools in conducting this sort of analysis, though it also makes clear that it does not require the use of any particular in-house or third-party software.

If you have any questions regarding the matters covered in this publication, please reach out to any of the lawyers listed below or your usual Davis Polk contact.

Paul Marquardt

+1 202 962 7156
paul.marquardt@davispolk.com

John B. Reynolds III

+1 202 962 7143
john.reynolds@davispolk.com

Will Schisa

+1 202 962 7129
will.schisa@davispolk.com

This communication, which we believe may be of interest to our clients and friends of the firm, is for general information only. It is not a full analysis of the matters presented and should not be relied upon as legal advice. This may be considered attorney advertising in some jurisdictions. Please refer to the firm's privacy notice for further details.

- ¹ OFAC defines the term "virtual currency" 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. OFAC also uses the term "digital currency," which includes virtual currency, as well as sovereign cryptocurrency and digital representations of fiat currency.
- ² Our prior client update on OFAC's "Framework for Compliance Program Commitments" is available [here](#).
- ³ For example, OFAC notes that unlisted virtual currency addresses that share a wallet with a listed virtual currency address may pose sanctions risk because the sharing of a wallet may indicate an association with a blocked person. It also suggests that virtual currency companies may consider conducting a historic lookback of transactional activity after OFAC lists a virtual currency address on the SDN List to identify connections to the listed address. A lookback could also identify connections to unlisted addresses that have previously transacted with the listed address, as such unlisted addresses could also pose sanctions risk depending on the nature of those transactions.