

## OFAC Publishes New Guidance for the Virtual Currency Industry

Written by Luciano Racco, Shrutih V. Tewarie, Anthony D. Mirenda

November 3, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) has published guidance to aid members of the virtual currency industry (ranging from tech companies to brokers to users) in complying with OFAC requirements. OFAC defines "virtual currency" to encompass non-sovereign, non-fiat currencies that can be used as a store of value or as a medium of exchange—a category inclusive of most cryptocurrencies, including common tokens such as Bitcoin or Ether. OFAC views the increased use of virtual currency in the world economy as presenting significant risks that sanctioned persons could exploit to evade sanctions and undermine U.S. foreign policy and national security interests.

OFAC's new guidance follows a number of recent virtual currency-related enforcement actions, including the [designation of cryptocurrency exchange SUEX OTC, S.R.O.](#) on OFAC's Specially Designated Nationals and Blocked Persons List (SDN List) on September 21, 2021 for facilitating financial transactions connected to ransomware operations. (For more on OFAC's guidance on ransomware, please see our [October 1, 2021 alert](#).) This increased attention comes on the heels of multiple recent Financial Crimes Enforcement Network (FinCEN) advisory notices related to illicit activities involving virtual currency. On October 28, 2021, the Financial Action Task Force issued [updated guidance](#) on a risk-based approach to virtual assets and virtual asset service providers to serve as a global benchmark. On November 1, 2021, the President's Working Group on Financial Markets provided a [report to Congress](#) on stablecoins (a form of virtual currency designed to maintain a stable value relative to a reference national currency), supporting the call for additional legislation to address, among other things, the illicit finance risks presented by stablecoins and other virtual currency. And in recent Senate testimony, Deputy Treasury Secretary Wally Adeyemo listed the growth of digital currencies as one of the primary challenges to the continued effectiveness of U.S. sanctions regimes. The uptick in enforcement actions can be understood as a part of a broader, whole-of-government effort to target vulnerabilities in the financial sector presented by virtual currency. The OFAC guidance is the latest in a number of recent signals from across the government that should put industry players on notice to expect increased scrutiny of virtual currency across the board.

### Traditional Compliance Obligations Apply to Virtual Currency

OFAC is responsible for the administration and enforcement of economic sanctions programs as applied against foreign countries, individuals, and other entities. This guidance emphasizes that the obligations triggered by U.S. sanctions apply with equal force to transactions conducted with virtual currency as they do to those made with traditional fiat currency.

As a result, much of OFAC's specific guidance aims to educate the virtual currency industry on various sanctions programs and details traditional best practices for ensuring compliance with U.S. sanctions. Broadly speaking, U.S. sanctions programs prohibit engaging in or facilitating (without a license) a wide range of transactions and activities, ranging from broad prohibitions on all unlicensed dealings with certain jurisdictions (like North Korea), to specific prohibitions on transactions or activities with listed individuals or involving certain identified property. Consequently, OFAC's basic compliance standards expect parties to have mechanisms to avoid, identify, evaluate and prevent such transactions and activities. Although OFAC may impose civil penalties based on the "strict liability" legal standard, OFAC generally takes into account whether an enterprise has implemented a reasonable compliance program and how it responds to discovery of an apparent violation in determining whether to impose a penalty, and, if so, its magnitude.

### Best Practices for the Virtual Currency Industry

Beyond putting the virtual currency industry on notice that OFAC is paying close attention to it, the guidance contains some specific best practices, including novel guidance on software tools that can enhance sanctions compliance. As in the past, OFAC recommends use of

geolocation tools including IP address blocking controls for any platform dealing with virtual currency, as a safeguard to avoid contact with sanctioned jurisdictions. However, for what appears to be the first time, the guidance acknowledges that a simple geography-based IP screen may be insufficient, recommending that companies also monitor for known virtual private network (VPN) addresses, to prevent users from masking their location. Companies in the virtual currency industry will need to carefully consider how to treat VPN use given that VPNs are frequently utilized by individuals and entities around the world for legitimate reasons, including as a security and privacy measure. OFAC also recommends screening for “improbable” IP logins, where an individual user repeatedly logs in from different, geographically distant locations within a short time. In making these specific recommendations, this publication provides the most detailed guidance to date with respect to VPN use on virtual currency platforms.

Additionally, OFAC recommends use of transaction monitoring and investigation software, making use of identifying information associated with virtual currency transactions. OFAC notes that it has been including certain known virtual currency addresses as identifying information for sanctioned persons on the SDN List. Best practices include not only monitoring and blocking transactions associated with listed addresses, but performing extra due diligence by monitoring suspicious virtual currency addresses that may be associated with known blocked persons. For example, OFAC recommends monitoring virtual currency addresses that share a wallet with listed addresses.

OFAC further details best practices associated with “Know Your Customer” (KYC) procedures. While such regulations have long been mandated for financial institutions, this guidance recommends their application to the virtual currency industry where users often place a premium on privacy and anonymity. OFAC characterizes a number of user behaviors that may be endemic to virtual currency as potential “red flags” including providing incomplete personal information, VPN use, or failing to respond to KYC requests.

### Implications for Virtual Currency Globally

The OFAC guidance marks an acceleration of recent trends in the U.S., with officials cracking down on use of virtual currency to evade traditional financial sector regulations. We expect U.S. regulators, including OFAC, FinCEN and other agencies, to continue to scrutinize and increase pressure on the industry. Whether attributable to the rise in ransomware attacks, or simply the increased popularity of cryptocurrencies, we expect that these moves will have ripple effects globally. Last month, speaking at a Center for a New American Security event, Deputy Secretary Adeyemo noted that the Treasury Department is aiming to work more with global partners, and is placing a high priority on multilateral designations related to cryptocurrencies. The President’s Working Group report on stablecoins reiterated that the Financial Action Task Force (FATF) will continue encouraging other countries to implement the FATF standards for virtual currency as part of global efforts to combat money laundering and the financing of terrorism. Going forward, we would expect to see additional activity from European regulators given that they have traditionally been vigilant in enforcing KYC regulations and may be under pressure to increase enforcement. We would also expect to see additional sanctions designations in the virtual currency industry, as well as high-profile prosecutions for sanctions violations and/or facilitation.

Companies with questions about this new OFAC guidance or how to ensure compliance with U.S. sanctions and export control regulations should contact a member of [Foley Hoag’s Trade Sanctions & Export Controls practice](#).

#### RELATED INDUSTRIES

- [Technology](#)

#### RELATED PRACTICES

- [Trade Sanctions & Export Controls](#)
- [Cybersecurity Incident Response](#)
- [Blockchain & Cryptocurrency](#)
- [Privacy & Data Security](#)
- [White Collar Crime & Government Investigations](#)

---

This communication is intended for general information purposes and as a service to clients and friends of Foley Hoag LLP. This communication should not be construed as legal advice or a legal opinion on any specific facts or circumstances, and does not create an attorney-client relationship.

United States Treasury Regulations require us to disclose the following: Any tax advice included in this document was not intended or written to be used, and it cannot be used, for the purpose of avoiding penalties under the Internal Revenue Code.

