



Financial Services & Products / International Trade & Regulatory ADVISORY ■

OCTOBER 22, 2021

How Can Companies Use OFAC's New Guidance on Virtual Currency?

by [Brendan Clegg](#), [Cliff Stanford](#), [Jason Waite](#), [Brian Frey](#), and [Matthew Bedford](#)

On October 15, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) released its [Sanctions Compliance Guidance for the Virtual Currency Industry](#). The Guidance defines virtual currency as a digital representation of value that is neither issued nor guaranteed by any jurisdiction and functions as a medium of exchange, a unit of account, or a store of value and distinguishes virtual currency from digital representations of fiat currency. OFAC describes the Guidance as a resource to help members of the industry comply with OFAC sanctions, and the document reflects the agency's recognition that virtual currencies are playing an increasingly important role in the global economy. Importantly, OFAC defines the virtual currency industry as including, at a minimum, technology companies, exchanges, administrators, miners, wallet providers, and users. As outlined by OFAC, the Guidance is intended to assist companies in this ever-growing industry with four specific objectives:

1. Evaluating sanctions-related risks within their lines of business.
2. Building a risk-based sanctions compliance program.
3. Protecting their business from sanctions violations and from intentional misuse of virtual currencies by malicious actors.
4. Understanding OFAC's recordkeeping, reporting, licensing, and enforcement processes.

Much of the Guidance serves as a distillation of the most relevant, and important, aspects of the U.S. sanctions framework, collected and sourced from OFAC's regulations, prior guidance, enforcement actions, and frequently asked questions. The Guidance serves as an excellent primer for companies unfamiliar with the features of the U.S. sanctions regime and covers, at a high level, notable aspects that could trip up new market entrants (for example, OFAC's 50 Percent Rule). Although much of the Guidance covers well-trod ground, it evidences a clear effort by the agency to put entities that operate in—or are considering operating in—the virtual currency space on notice, likely signaling that the agency plans to ratchet up its focus on the industry in the coming months. The Guidance also represents an attempt to establish defined terms in an area that remains largely unregulated.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

In light of the anticipated uptick in regulatory scrutiny, the Guidance provides companies in the industry valuable insight into the agency's views on two topics that should be top of mind: (1) sanctions screening procedures; and (2) the broader sanctions compliance framework. By adhering to the recommendations in the Guidance, companies in this space may be able to avoid—or, if necessary, mitigate—compliance issues that may arise.

Sanctions Screening Procedures

While the new Guidance recaps much of the agency's prior commentary on sanctions screening, it dedicates nearly a page to its recommended best practices for virtual currency companies to incorporate geolocation tools and IP address blocking controls. Specifically, the Guidance states that companies with strong sanctions compliance programs "should be able to use geolocation tools to identify and prevent IP addresses that originate in sanctioned jurisdictions from accessing [their] website[s] and services" for prohibited activity, if such activity is not authorized or exempt. The Guidance points out analytic tools that can identify IP misattribution, such as diagnosing improbable login patterns. OFAC's decision to single out these tools as examples is a strong indication that the agency views them as important compliance controls for virtual currency companies.

Beyond the use of more sophisticated tools, however, OFAC also emphasizes the importance of thoughtfully integrating more basic due diligence information into location-related screening procedures. The Guidance points out that location data can come from such varied sources as customer or counterparty information, email addresses, invoices, or the transactions themselves. While the purpose of the collection of these types of information may not have been sanctions related, OFAC recommends that companies merge such information into their screening processes, taking advantage of these additional data points to enhance the robustness of their screening. The Guidance includes a reminder that in the past, the agency has initiated enforcement actions within the industry for failure to prevent users in sanctioned jurisdictions from using companies' platforms, and these failures were premised, in part, on a failure to incorporate geolocation information *in the companies' possession*. Should a compliance issue arise down the road, companies that incorporate such tools and processes into their sanctions compliance program should have a stronger argument before the agency that they tried to use the information they had to block prohibited transactions.

The Guidance also notes that since 2018, OFAC has included known virtual currency addresses as identifying information for individuals listed on the agency's Specially Designated Nationals and Blocked Persons (SDN) List. Beyond screening all virtual currency addresses associated with a particular transaction against the SDN List (as for any type of identifying information collected or in the companies' possession related to the transaction), the Guidance also suggests that companies in the industry may be able to identify *other* addresses that may be associated with designated persons, or that pose sanctions risk, even if those other addresses are not listed. OFAC observes that unlisted addresses that share a wallet with a listed address may pose a sanctions risk because of the potential association with a blocked person. The Guidance does not offer suggestions for how companies can resolve these types of associational red flags.

In addition, the Guidance suggests companies should consider historical lookbacks after OFAC updates the SDN List to designate new virtual currency addresses to identify connections between the listed address and the unlisted addresses. The Guidance is not clear on the purpose of such lookbacks, but the purposes could include enhancement of proprietary internal screening lists or information sharing with industry partners and regulators. However, companies with strong screening programs typically focus on actively preventing future transactions with persons or addresses designated at the time of the transaction. A system of ongoing lookbacks focused on transactions with persons or addresses that were not designated at the time of the transactions could divert valuable resources from ongoing compliance efforts. The agency points out that blockchain analytics tools could be deployed to perform these tasks.

Alston & Bird has advised our clients in the cryptocurrency space on utilization of these tools, which can greatly assist companies in identifying and mitigating sanctions risks.

The Broader Sanctions Compliance Program Framework

The Guidance sets out OFAC's encouragement to all companies in the virtual currency industry, as well as financial institutions and service providers with exposure to the industry, to develop and implement a tailored, risk-based sanctions compliance program that aligns with its [Framework for OFAC Compliance Commitments](#). Beyond the emphasis on each of the component parts of this framework, the Guidance reflects two important observations from OFAC related to entities' sanctions compliance programs.

First, the Guidance reveals OFAC's long-running observation that participants in the virtual currency industry implement programs "months, or even years," after commencing operations, a delay that exposes the entities to a "wide variety" of potential sanctions risks. The Guidance states OFAC's view that it is "never too soon" to evaluate potential sanction risks, and it recognizes that in the virtual currency industry the appropriate types of internal controls for a given company depend on its activities and operations and the risks that arise from them. In addition, OFAC suggests that these companies should explicitly consider sanctions compliance during technology development and before launching a new product.

Second, the same page of the Guidance on "Management Commitment" couples this view with a list of steps that senior industry managers can consider to "demonstrate their support for sanctions compliance." Among those steps listed are the deployment of "adequate" resources, delegation of a "compliance unit" with autonomy and authority, and appointment of a dedicated compliance officer with the "requisite technical expertise."

Taken together, OFAC's discussion of how management can demonstrate a commitment to sanctions compliance displays a clear agency emphasis on the early adoption of a compliance program with sufficient resources, expertise, capability, and independence to ensure that sanctions compliance is an enterprise-wide priority. Although dedication of the requisite level of resources at an early stage may be difficult for companies in this space, especially startups, installation of an experienced, knowledgeable compliance officer before the launch of the company's operations or products should demonstrate a company's recognition of the importance of sanctions compliance. Moreover, a dedicated compliance officer can help build out the contours of the framework to meet OFAC's other expectations for management commitment—such as policies and procedures, technology integration, and expansion of a more complete compliance unit—as the company continues to expand and grow. This will allow the company to avoid playing catch-up once it is already too late. If the sanctions risks posed by a company's activities warrant expenditure of resources, the Guidance illustrates that the early-stage build-out of the compliance program will help assuage OFAC if problems are encountered later.

Finally, we note one potential tension between the Guidance and the Financial Crimes Enforcement Network's (FinCEN) regulations implementing the Bank Secrecy Act (BSA). FinCEN's 2013 and 2019 guidance on convertible virtual currencies (CVCs) makes clear that some companies' business models involving CVCs will render those entities money transmitters and, therefore, money services businesses (MSBs) subject to the BSA. Unlike some other types of covered financial institutions, MSBs are not formally required to implement a customer identification program (CIP), although many MSBs may in fact adopt and deploy a CIP that mirrors the requirements of, say, a bank CIP. In the Guidance, however, OFAC suggests that it is a best practice for virtual currency companies to obtain information about their customers at onboarding, including the four core pieces of customer data required by the CIP rule. Whether virtual currency companies that are MSBs for BSA purposes feel obligated to collect such information from

customers at onboarding to comply with the Guidance—even if not a formal legal requirement for anti-money laundering regulatory purposes—could be an interesting compliance quandary for companies to face as they digest OFAC's newest issuance.

* * *

The virtual currency industry continues to be the subject of intense scrutiny as several federal regulators circle, and debates over how the industry should be regulated proliferate. As covered in our [Privacy, Cyber & Data Strategy Blog](#), the Department of Justice recently announced a new cryptocurrency enforcement team. In addition, the issuance of the Guidance coincides with the release of the Treasury Department's [2021 Sanctions Review report](#) highlighting that digital currencies and alternative payment platforms potentially reduce the efficacy of American sanctions. Alston & Bird regularly represents a wide variety of companies on OFAC and sanctions-related issues and counsels entities throughout the virtual currency industry on regulatory, compliance, and enforcement matters. Should you have any questions about the Guidance, or the regulatory regimes of OFAC or FinCEN, please do not hesitate to reach out to any of the authors of this advisory.

You can subscribe to future *Financial Services & Products* and *International Trade & Regulatory* advisories and other Alston & Bird publications by completing our [publications subscription form](#).

If you have any questions or would like additional information please contact your Alston & Bird attorney or any of the following:

Clifford S. Stanford
404.881.7833
cliff.stanford@alston.com

Brendan Clegg
202.239.3237
brendan.clegg@alston.com

Jason M. Waite
202.239.3455
jason.waite@alston.com

Matthew Bedford
202.239.3169
matthew.bedford@alston.com

Brian D. Frey
202.239.3067
brian.frey@alston.com

ALSTON & BIRD

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2021

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: 3700 Hulen Street ■ Building 3 ■ Suite 150 ■ Fort Worth, Texas, USA, 76107 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 5th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333