Cleary Foreign Investment and International Trade Watch

OFAC Issues Sanctions Guidance to Virtual Currency Industry

By Abena Mainoo, Chase D. Kaniecki, Michael G. Sanders, John Lightbourne & William S. Dawley on October 22, 2021

On October 15, 2021, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") issued "**Sanctions Compliance Guidance for the Virtual Currency Industry**" (the "Guidance"). The Guidance follows recent guidance and advisory letters directed to the virtual currency industry relating to the risk of facilitating ransomware payments[1] and is OFAC's most comprehensive virtual currency-specific advisory to date. In particular, the Guidance directly addresses some simpler interpretive questions, discusses sanctions compliance programs and "best practices," and provides hints about OFAC's enforcement priorities going forward.

The Guidance, along with OFAC's recent enforcement activity in the virtual currency space, confirms that OFAC is focused on market participants' compliance with applicable U.S. sanctions laws and regulations, despite the novel nature of the underlying technologies. To that point, the advisory is addressed to the "virtual currency industry," which OFAC broadly defines to include technology companies, exchangers, administrators, miners, wallet providers, and users ("Market Participants"). This is a more expansive group (e.g., miners or validators) than OFAC has historically focused on in enforcement actions or its FAQs concerning virtual currency activities.

Provided below is a summary of some key issues addressed in the Guidance.

OFAC's Broad Jurisdiction

The Guidance reminds Market Participants that U.S. sanctions laws apply to all U.S. citizens and lawful permanent residents wherever located, all individuals and entities located within the United

States and all entities organized under the laws of the United States or any jurisdiction of the United States, including foreign branches of those entities. In addition, certain activities by non-U.S. persons that involve a U.S. nexus, such as U.S. persons or good or services exported from the United States, may be subject to sanctions restrictions.

Blocking Virtual Currency

The Guidance clarifies that to "block" virtual currency, generally the Market Participant must deny all parties access to the blocked virtual currency and, like fiat currency, report the blocked virtual currency to OFAC. However, Market Participants are not required to convert the virtual currency into fiat currency or, unlike fiat currency, hold the virtual currency in an interest-bearing account.

In some instances, "blocking" virtual currency may be difficult, both conceptually and technically. This is especially the case in the context of automated smart contracts or underlying network protocols that automatically make disbursements of virtual currency in certain scenarios, such as network generated staking rewards made to users that "delegate" assets to on-chain validators. However, as a result of developments such as token standards that allow for increased restrictions on transferability and products from blockchain analytics firms that help developers incorporate sanctions-related screenings and monitoring into virtual currency networks and decentralized applications, there are more opportunities for virtual currency networks to incorporate controls responsive to OFAC's concerns than we have seen in the past. In addition, in our experience, certain state regulators often require the ability to "freeze" virtual currencies if issued by regulated institutions. Thus, while the Guidance appears to more cleanly apply to payment processors, exchanges and similar intermediaries, Market Participants and developers more generally should take heed and consider opportunities to incorporate sanctions-related controls into their virtual currency activities and projects.

Compliance Programs and Enforcement Risk

The Guidance reiterates that OFAC's "**Framework for OFAC Compliance Commitments**" (the "Framework"), which details OFAC's expectations for risk-based sanctions compliance programs, is applicable to Market Participants in the virtual currency industry. The Framework highlights OFAC's expectation that parties have formal, written compliance programs, including the need for management's commitment to sanctions compliance, risk assessments, internal controls, periodic testing and auditing and sanctions-related training.

Sanctions compliance programs should be risk-based and tailored to the specific company or end user, informed by the entity's risk assessment. Factors to consider in developing a sanctions compliance program include the types of products and services offered, the geographic locations served, a firm's size and sophistication, and the types of customers and counterparties.

In addition to universal "best practices" such as counterparty screening and "know your customer" ("KYC") procedures, the Guidance has both specific and implicit advice for developing an effective sanctions compliance program in the virtual currency space, including that Market Participants adopt strong sanctions policies before providing services or products to customers (which OFAC notes many do not). Highlights include:

- Geolocation and other location-based information: The Guidance reinforces statements made in past enforcement actions suggesting that OFAC views basic geolocation and IP blocking as a minimum expectation for sanctions compliance programs. Consistent with past enforcement actions, the Guidance emphasizes the importance of geolocation and IP blocking tools that can identify parties operating in sanctioned jurisdictions, including tools that can screen for IP misattribution (for example, the use of VPN services to disguise a party's true location). OFAC also encourages and expects participants in the virtual currency industry to screen other information they acquire to detect activity involving sanctioned jurisdictions, with location information acquired for other purposes serving "double-duty" for transaction monitoring and sanctions screening programs. This was a specific issue OFAC highlighted in its recent settlement with BitPay, Inc. There, OFAC alleged that Bitpay, Inc. failed to screen location data regarding its merchant customers' end users that was available on invoices, and consequently processed payments on behalf of end users located in sanctioned jurisdictions.[2]
- Transaction monitoring and investigation: The Guidance suggests that in-house or third party monitoring services "can be helpful tools," implying that OFAC views the use of blockchain analytics services as a "best practice." The Guidance notes that dealing with addresses that have transacted with sanctions-listed addresses could "pose sanctions risk" and "blockchain analytics tools [may] help identify and mitigate these sanctions risks." Consistent with our experience, the Guidance suggests that OFAC expects Market Participants to screen transactions at a minimum against its sanctions lists, including digital wallet addresses. Blockchain analytics firms and their blockchain tracing tools and proprietary database of digital wallet addresses with links to sanctioned addresses may be particularly helpful in performing this and additional screening, assisting Market Participants to both prevent sanctions violations and receive credit from OFAC

when violations are identified. OFAC itself appears to have contracted with blockchain analytics firms to investigate potential sanctions violations.[3]

- KYC: OFAC recommends the adoption of certain KYC processes—and provides examples of specific information that may be collected—as a "best practice."[4] Notably, many Market Participants are regulated financial institutions or money services businesses subject to regulation by the U.S. Department of the Treasury's Financial Crimes Enforcement Network under the Bank Secrecy Act ("BSA") or otherwise subject to the BSA and required to adopt anti-money laundering programs that include KYC policies and procedures. However, OFAC lists some types of information to consider collecting as part of KYC that may not currently be necessary to collect under the BSA, particularly with respect to money services businesses. Additionally, some Market Participants, such as mining pools and certain end users, are likely not subject to the BSA. The Guidance suggests that OFAC expects Market Participants that otherwise do not have a regulatory obligation to perform KYC screening under applicable anti-money laundering laws to nonetheless adopt KYC procedures as part of their compliance with sanctions laws.

- Red flags: The Guidance provides specific examples of "red flags" that may indicate a sanctions nexus, which Market Participants should incorporate into their sanctions compliance programs.[5]

- Reporting and investigating potential violations: The Guidance also discusses OFAC's recommendations for addressing potential sanctions violations by Market Participants. OFAC encourages (1) voluntarily self-disclosing violations to OFAC, (2) performing an analysis to determine the "root cause" of the violations, (3) remediating identified weaknesses and implementing new controls to prevent future violations,[6] and (4) conducting a historical lookback of transactional activity to identify additional concerns or violations. OFAC may consider a party's remediation measures in response to violations in determining whether to pursue an enforcement action, and voluntarily disclosing a violation may result in a 50 percent reduction in the base amount of any proposed civil penalty.

The Guidance does not specifically address the application of U.S. sanctions laws to developments in the decentralized finance space, despite other U.S. and international regulatory bodies, such as the Financial Action Task Force, beginning to grapple with the implications of decentralized smart contracts and programs providing financial services without a centralized party or administrator. For

example, the Guidance does not answer the question what does it mean for a U.S. person to come into possession of virtual currency in the context of launching a decentralized app.

Conclusion

While the Guidance reflects a concerted effort to consolidate past guidance and apply it to the virtual currency industry, the recommendations themselves are not particularly novel or surprising. Nonetheless, it reinforces for Market Participants the importance of having an effective sanctions compliance program, which OFAC takes into account when considering whether to pursue an enforcement action in connection with sanctions violations. Given the strict liability nature of U.S. sanctions and the increased scrutiny on virtual currency transactions, implementation of compliance "best practices" is, as a practical matter, crucial in mitigating enforcement risks and could be the difference between a private cautionary letter with no penalty and a public civil penalty. In our experience, OFAC is less likely to impose penalties on Market Participants that voluntarily self-disclose potential sanctions violations to OFAC if such parties have strong compliance programs and implement "best practices."

---

[1] For further discussion of these recent developments, see ***OFAC Updates Ransomware Advisory and Sanctions Virtual Currency Exchange***.

[2] For further discussion of the BitPay, Inc. settlement, see ***OFAC Settles with Digital Currency Payment Processor for Sanctions Violations***.

[3] OFAC issued a public **notice** requesting bids for blockchain analytics tools in May 2021, and the press **reports** at the time indicated that OFAC had selected Chainalysis from the bidding process. Chainalysis has also publicly **stated** in the past that both OFAC and the U.S. Department of Justice used its tool in connection with a civil action against two Chinese nationals alleged to have assisted a North Korean-aligned group launder stolen virtual currencies.

[4] Specifically, OFAC recommends collection of identification information similar to what would be collected for identity verification purposes as part of an anti-money laundering compliance program, as well as IP addresses, emails and bank information. Higher-risk customers may warrant additional due diligence.

[5] Examples of "red flags" include providing inaccurate or incomplete customer identification information, or otherwise being non-responsive to requests for identification or transaction information; using an IP address or VPN connected to a sanctioned jurisdiction; and attempting to transact with a virtual currency address associated with a blocked person or sanctioned jurisdiction.

[6] OFAC lists the following specific remedial measures companies have taken in response to enforcement actions: (1) implementing IP address blocking and email-related restrictions for sanctioned jurisdictions, (2) instituting an OFAC-related training program for employees, (3) creating a keywords list of a sanctioned jurisdiction's cities and regions to be used when screening KYC information, (4) conducting additional sanctions compliance training for all relevant personnel, (5) reviewing and updating end user agreements to include information about U.S. sanctions requirements, (6) hiring additional compliance staff and a dedicated chief or sanctions compliance officer, and (7) conducting retroactive batch screening of all users.

Cleary Foreign Investment and International Trade **Watch**