Virtual Currencies & U.S. Sanctions

Co-Authored by Jennifer Diaz and Sharath Patil*

*Jennifer Diaz is President of Diaz Trade Law based in Miami, FL. Sharath Patil is an Associate Attorney at Diaz Trade Law based in Washington, DC.

Introduction

As virtual currencies gain popularity and are touted as a legitimate, reliable, and potentially useful medium of exchange, there is significant concern about how the new technology will be effectively regulated. Virtual currencies have vast implications in a wide array of regulatory areas including privacy, tax, and securities, just to name a few. This article will focus on virtual currencies scrutiny under U.S. sanctions programs administered by the U.S. Treasury Department’s Office of Foreign Assets Control (“OFAC”) given the potential national security and foreign policy threats posed by their increasingly widespread use.

Threats to Existing U.S. Sanctions Programs from Virtual Currencies

On October 18, 2021, the U.S. Treasury Department warned that digital currencies posed a threat to U.S. sanctions programs and that U.S. sanctions programs must be modernized to maintain their effectiveness. In a report that evaluated the state of U.S. sanctions programs in the preceding six months, the Department found that “Digital currencies... potentially reduce the efficacy of American sanctions” and that “…if left unchecked, these digital assets and payment could harm the efficacy of our sanctions.” In terms of solutions, the report emphasized the importance of increased outreach and engagement with stakeholders in order to ensure that sanctions are easily understood, enforceable, and adaptable. Furthermore, the report recommended that the U.S. Treasury Department “[deepen] its institutional knowledge and capabilities in the evolving digital assets and services space...” While virtual currencies have been identified as a serious potential threat to existing U.S. sanctions programs, OFAC has recently issued significant guidance on how virtual currencies will be regulated moving forward.

Definitions

The following are definitions of key terms pertaining to virtual currencies.

- **Blockchain** – Blockchain is a shared, immutable ledger that facilitates the process of recording transactions and tracking assets in a business network. Virtually anything of value can be tracked and traded on a blockchain network.

- **Cryptocurrency** – Cryptocurrency is virtual currency that implements cryptography technology to secure and authenticate currency transactions. Cryptocurrencies
depend on blockchain networks. Cryptocurrency is generally considered a subset of 
virtual currency.

- **Digital Currency** – A form of currency that is available only in digital or electronic 
form and do not require intermediaries. All cryptocurrencies are digital currencies, 
but it is not vice versa. Other names are digital money, electronic money, electronic 
currency, or cybercash. Examples of digital currency include sovereign 
cryptocurrency, virtual currency (non-fiat), and a digital representation of fiat 
currency.

- **Fiat Currency** – Fiat currency is currency that is backed by the public's faith in the 
government or central bank that issued it and (unlike a commodity currency) is not 
linked to a price of a commodity such as gold or silver. Fiat currencies can be digitally 
represented as digital currency.

- **Virtual Currency** – According to OFAC, it is a digital representation of value that 
functions as (i) a medium or exchange; (ii) a unit of account; or (iii) a store of value; 
and is neither issued nor guaranteed by any jurisdiction. A virtual currency is a subset 
of a digital currency.

**U.S. Sanctions Policies for Virtual Currencies**

OFAC administers and enforces a broad range of sanctions programs in order to further U.S. 
foreign policy and national security goals. These sanctions programs vary greatly in scope, 
and include targeted foreign countries and regimes, terrorist organizations, international 
narcotics traffickers, proliferators of weapons of mass destruction, and other threats to the 
national security, foreign policy, or economy of the United States.

In October 2021, OFAC issued Sanctions Compliance Guidance for the Virtual Currency Industry. 
In its publication, OFAC underscored that the growing prevalence of virtual currency as a 
payment method creates an increased risk of sanctions violations. Accordingly, numerous 
parties in the virtual currency industry including exchange platforms, miners, wallet 
providers, and users are implicated by U.S. sanctions laws.

Interestingly, OFAC notes that sanctions compliance obligations apply equally to transactions 
involving virtual and traditional fiat currencies, and that virtual currency industry members 
are responsible for ensuring that they do not engage in prohibited transactions. Generally, 
OFAC's jurisdiction applies to:

1. non-U.S. persons while in the United States,
2. U.S. citizens and permanent residents wherever located,
3. U.S. entities and foreign branches, and

**OFAC Enforcement & Virtual Currencies**
Violations of sanctions can carry heavy civil penalties or even criminal liability. Penalties are assessed per violation and vary depending on the specific law violated. Adjusted maximum penalties for some sanctions violations are listed below:

- Clean Diamond Trade Act – $14,074
- Trading with the Enemy Act – $91,816
- Foreign Narcotics Kingpin Designation Act – $1,548,075
- International Emergency Economic Powers Act – Greater of $111,562 or twice the amount of the underlying transaction

A key compliance consideration for parties in the virtual currency space is the potential for violations to quickly compound. The penalties listed above are “per violation.” When virtual currency-related sanctions violations occur, it is likely that numerous transactions were involved rather than a single transaction. OFAC generally exercises discretion in determining whether a set of similar transactions constitutes a single violation or multiple. If OFAC deems that a series of prohibited transactions constitutes many different violations, the potential civil and criminal liability can quickly skyrocket. This is demonstrated in the below case studies:

- **OFAC targets Russian virtual currency exchange SUEX OTC, S.R.O.** – On September 21, 2021, OFAC designated SUEX to the Specially Designated Nationals list after the Russia-based virtual currency exchange was found to play a part in facilitating illicit financial transactions for ransomware actors. This was the first time that a virtual currency exchange was designated on the Specially Designated Nationals list.

- **BitPay, Inc. settles for $507,375 with OFAC** – On February 18, 2021, OFAC entered into a $507,375 settlement with BitPay, an Atlanta, GA-based company, for 2,102 apparent violations of multiple sanctions programs. Specifically, BitPay failed to prevent persons located in the Crimea region of Ukraine, Cuba, North Korea, Iran, Sudan, and Syria from transacting with merchants in the United States and elsewhere using digital currency on BitPay’s platform. BitPay had reason to know where these users were based on their IP addresses.

- **BitGo, Inc. settles for $98,830 with OFAC** – On December 30, 2020, OFAC entered into a $98,830 settlement with BitGo, a Palo Alto, CA technology company, for 183 apparent violations of multiple sanctions programs. Specifically, BitGo failed to prevent persons located in the Crimea region of Ukraine, Cuba, Iran, Sudan, and Syria from using its secure digital wallet management service. BitGo had reason to know where these users were located based on their Internet Protocol (IP) addresses.

- **OFAC Sanctions Individuals for Laundering Cryptocurrency for Lazarus Group** – On March 2, 2020, OFAC sanctioned two Chinese nationals involved in laundering stolen cryptocurrency from a 2018 cyber intrusion against a cryptocurrency exchange. The cyber intrusion was linked to Lazarus Group, a U.S.-designated North Korean state-sponsored malicious cyber group.
**Best Practices**

Any party involved in the virtual currency space including exchange platforms, miners, wallet providers, and users should create a sanctions compliance program. A sanctions compliance program is important because it:

- Helps ensure that all employees understand U.S. sanctions laws and reinforces internal policies and procedures,
- Demonstrates to OFAC that your business is proactive about sanctions compliance, and
- Can help avoid or mitigate costly penalties and potential criminal liability.

Like all sanctions compliance programs, parties in the virtual currency industry should ensure their sanctions compliance program includes:

- Management commitment to compliance
- Risk assessment
- A proactive mechanism for screening violative transactions
- Auditing and internal monitoring
- Recordkeeping
- Handling sanctions violations when they do occur and implementing corrective actions
- Seeking OFAC authorization when necessary

Although sanctions compliance in the virtual currency industry is similar to sanctions compliance generally, parties in the virtual currency industry should be well aware of both the unique sanctions implications for their transactions and the tools available to ensure compliance. OFAC emphasizes the use of tools such as (1) geolocation tools, and (2) transaction monitoring and investigation software.

- **Geolocation Tools** – Parties in the virtual currency industry have the ability to use geolocation tools to identify and prevent IP addresses that originated in sanctioned jurisdictions from accessing a company's website for prohibited activities.
- **Transaction Monitoring and Investigation Software** – Parties in the virtual currency industry have access to software / technology that can prevent transfers to addresses associated with sanctioned persons. Furthermore, virtual currency companies often have the ability to automate their screening processes to ensure that individuals and entities designated on the SDN list do not have the ability to engage in transactions.

**Conclusion**
U.S. sanctions laws are, by their nature, dynamic and subject to change. U.S. sanctions policies reflect changes in global crime and geopolitics and strive to respond quickly to emerging threats. The increased adoption of virtual currencies in their various forms simultaneously presents (1) a threat to the effectiveness of current U.S. sanctions programs, and (2) increased scrutiny as regulators grapple with how best to ensure the virtual currency industry adheres to U.S. sanctions laws. U.S. virtual currency companies should begin by understanding the relevance of U.S. sanctions laws to their operations, and then develop a robust sanctions compliance plan to minimize the risk of sanctions violations.