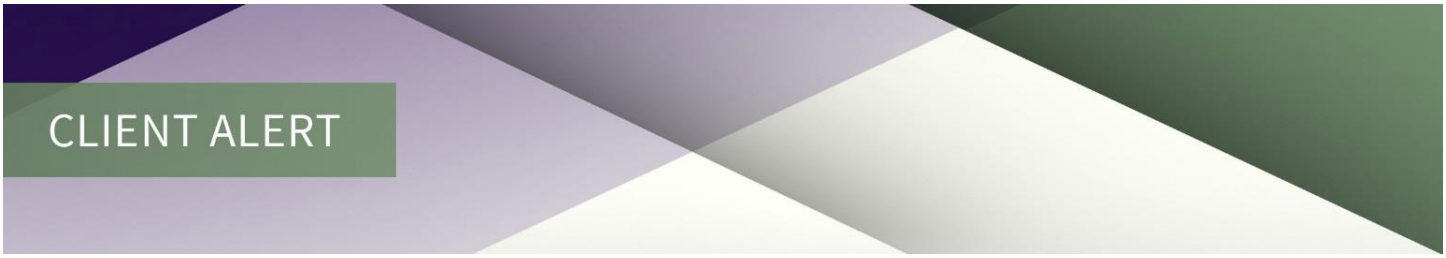

OFAC Sanctions Considerations for the Crypto Sector

September 29, 2021

AUTHORS

Britt Mosman | David Mortlock | Elizabeth P. Gray | J. Christopher Giancarlo
Samuel Hall

In recent years, the U.S. government has become increasingly focused on regulating the use of virtual currencies as a means of addressing a host of financial crimes and malign activities. As entities and individuals ("persons") in this space find themselves subject to various, sometimes overlapping regulatory regimes, the compliance environment has become increasingly treacherous. One area of particular concern for those dealing with cryptocurrencies is U.S. economic sanctions, as is evidenced by the recent settlement between the Treasury Department's Office of Foreign Assets Control ("OFAC") and BitPay Inc. ("BitPay"), discussed below. Indeed, sanctions hold some of the most complicated compliance issues in one hand, and some of the largest penalties in the other, and they do not always—or perhaps rarely—fit cryptocurrency transactions neatly.

This alert provides an overview of sanctions compliance principles for the cryptocurrency industry and discusses some key issues of which persons in the crypto space should be mindful, including:

- Sanctioned coins, persons, and regions;
- Restricted transactions; and
- Recommendations for compliance.

As this alert makes clear, some of the relevant prohibitions remain ambiguous and leave significant questions unanswered. In turn, some crypto transactions and related regulations may warrant license and guidance requests to OFAC or even legal challenges, including Administrative Procedure Act ("APA") challenges, in U.S. courts to resolve those ambiguities. But at a minimum, there are certain basic steps that should be taken to comply with U.S. sanctions.

a. Overview of Sanctions Compliance Issues for Cryptocurrency Industry

OFAC administers and enforces various economic sanctions programs against geographical regions, governments, groups, and individuals. OFAC regulations generally prohibit U.S. persons[1] from engaging in transactions, directly or indirectly, with geographical regions or persons targeted by sanctions. In addition, U.S. persons are generally prohibited from "facilitating" or assisting the actions of non-U.S. persons that would be prohibited for U.S. persons to perform directly due to U.S. sanctions. Under OFAC's definition of U.S. person, crypto exchanges, technology companies, payment processers, and administrators located or organized in the United States are U.S. persons, as are any users of digital currencies who are U.S. citizens or "green card" holders, regardless of where such individuals are located. As a result, those persons are directly restrained by U.S. sanctions from generally providing benefits to a sanctioned jurisdiction or engaging in any transaction involving a designated person.

OFAC prohibitions apply equally to all U.S. persons, from traditional financial institutions to the cryptocurrency industry. And the stakes are high. Violations of sanctions can carry both civil and criminal penalties, with the latter ranging up to $1 million and/or 20 years in prison *for each violation*, a terrifying metric for those that process thousands of transactions a day. What is more, OFAC may impose civil penalties for sanctions violations based on strict liability, meaning that a U.S. person may be held civilly liable even if it did not know or have reason to know it was engaging in a transaction with a person that is prohibited under OFAC-administered sanctions.[2]

To add to the risks for the cryptocurrency industry, OFAC has made clear that preventing sanctions evasion through cryptocurrency is a high priority for the agency, and it intends to use its sanctions authorities to counter the use of cryptocurrencies by sanctions targets and other malicious actors who abuse cryptocurrencies and emerging payment systems.[3] Moreover, OFAC has emphasized that U.S. persons that are engaged in "online commerce or process transactions using digital currency, are responsible for ensuring that they do not engage in unauthorized transactions

---

1 U.S. persons are defined to include (i) United States citizens and permanent resident aliens, wherever located; (ii) all entities organized in the United States (including their foreign branches); and (iii) all individuals, entities and organizations actually located in the United States. For the U.S. sanctions against Cuba and Iran, all entities owned or controlled by U.S. persons, wherever organized or doing business (including foreign subsidiaries), are also generally required to comply with such sanctions.

2 That said, OFAC generally considers knowledge, intent, recklessness, and negligence when determining which violations warrant an enforcement action.

3 *See, e.g.*, OFAC FAQ No. 561.

prohibited by OFAC sanctions[.]"[4] Indeed, we are already starting to see enforcement actions brought by OFAC against providers of cryptocurrency services and anticipate seeing more.[5]

Given these potential penalties and the U.S. government's current focus on the use of cryptocurrencies to engage in illicit activity, including evading OFAC sanctions requirements, crypto-industry participants should be aware, at a minimum, of a few broad categories of transactions that may pose risks.

b. Blocked Coins

Fortunately, there are some clear rules of the road. Certain cryptocurrencies have been blocked outright, and U.S. persons are prohibited from dealing in them or facilitating any dealings in them. In March 2018, President Trump issued Executive Order 13827 to prohibit U.S. persons from dealing in digital currencies that were issued by, for, or on behalf of the Government of Venezuela after January 9, 2018. The Order was a response to the Maduro regime's launch of its own sovereign cryptocurrency, the "Petro," in part to circumvent U.S. sanctions.

As a result of Executive Order 13827, no U.S. person may take part in any transaction that utilizes digital currencies put out by the Venezuelan government, such as "Petro" and "Petro Gold."[6] This Order carries increased importance as recent reporting suggests that the Maduro regime aims to direct significant future transactions toward government-backed digital coins.[7]

c. Blocked Persons

Although broad restrictions on specific coins are fairly easy to avoid, others are far less so. The more difficult restrictions for compliance purposes center around blocked persons. As noted above, U.S. persons are prohibited from engaging in transactions involving the property and interests in property of blocked persons, regardless of whether the transactions are denominated in traditional fiat or digital currency. OFAC appears to be focusing its efforts to crack down on prohibited transactions using cryptocurrencies that involve so called "Specially Designated Nationals and Blocked Persons" or "SDNs." To that end, OFAC has taken a number of actions in which it has identified digital currency addresses associated with targeted SDNs and added the addresses to the OFAC-administered "SDN List," thereby making that blockchain attribution public. This allows crypto sector participants to more easily screen for digital currency payments associated with SDNs and to conduct lookbacks on prior activity. OFAC will likely continue to add digital currency addresses to the

4 OFAC FAQ No. 560.

5 *See* U.S. Department of the Treasury, *Enforcement Release: OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions*, Feb. 18, 2021, *available online* here.

6 OFAC FAQ No. 564.

7 *See, e.g.,* Felipe Erazo, "Venezuelan President Maduro Promises 2021 Will Be the Year to Boost Usage of Petro," Bitcoin News (Jan. 15, 2021), *available online* here.

SDN List, especially given the lack of traditional identifiers (such as names and dates of birth) in the digital currency context.

The scope of prohibited crypto transactions involving SDNs is extremely broad. Guidance from OFAC shows that blocking restrictions will extend to indirect benefits to, or involvement of, blocked entities in a transaction or dealing, including bans on "enter[ing] into contracts that are signed by" a blocked entity[8] and participating in negotiations with a blocked entity.[9] This illustrates how essentially *any* transactions—from simple transfers of digital coins to smart contracts—involving cryptocurrencies associated with an SDN, or with an entity 50% or more owned by an SDN, [10] and a U.S. person can result in a sanctions violation. What is more, even if a crypto address is not known to be associated with an SDN at the time of a transaction, transactions involving an address that is later linked to an SDN could be considered a violation, so long as the transaction occurred after the SDN was designated, given the strict liability nature of the OFAC sanctions regime (discussed above). Similarly, a digital asset in which a blocked person has an interest continues to be "blocked" property, regardless of the number of transfers away from a known blocked address. Transactions involving Mixers, Tumblers, and Chain Hopping, where the parties involved are obscured, are therefore at an increased risk.

Ransomware payments are a good example of how these sanctions-related implications present themselves in the market. Until recently, insurance providers have been generally willing to agree to reimburse ransomware payments, often in the form of cryptocurrencies, due to the enormous cost to rebuild systems and recover lost data following a ransomware attack. However, OFAC has designated several companies and actors associated with certain malware, including those associated with Cryptolocker, SamSam, WannaCry 2.0 and Dridex, and OFAC recently designated SUEX OTC, S.R.O. ("SUEX"), "a virtual currency exchange, for its part in facilitating financial transactions for ransomware actors, involving illicit proceeds from at least eight ransomware variants."[11] In turn, ransomware payments involving these persons (or any sanctioned jurisdiction) are prohibited.[12] And as a result, many insurance companies have begun adding explicit exclusions to their cyber policies for ransomware payments to sanctioned actors or actors located in sanctioned jurisdictions. Given how many ransomware attacks carry "signatures" or other means to ascertain what actor is behind the attack, ransomware payments can carry significant risks under U.S. sanctions especially when the victim knows the threat actor or does not take reasonable steps to ascertain who the threat actor is. OFAC guidance encourages victims and those involved with addressing ransomware attacks to contact law enforcement or other Government agencies—such

8 *See* OFAC FAQ No. 400.

9 *See* OFAC FAQ, Nos. 505 and 547; *see also* OFAC, "Revised Guidance on Entities Owned by Persons Whose Property and Interests in Property Are Blocked" (August 13, 2014), *available online* here (stating that U.S. persons "may not procure goods, services, or technology from, or engage in transactions with, *a blocked person directly or indirectly (including through a third-party intermediary)*" (emphasis added)).

10 *See* U.S. Treasury Department, Revised guidance on entities owned by persons whose property and interest are blocked, *available online* here.

11 Treasury Department, *Treasury Takes Robust Actions to Counter Ransomware* (Press Release) Sep. 21, 2021, *available online* here.

12 *See, e.g.,* Treasury Department, *Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses* (Press Release) Nov. 28, 2018, *available online* here.

as the Cybersecurity and Infrastructure Security Agency ("CISA"), the U.S. Department of the Treasury' s Office of Cybersecurity and Critical Infrastructure Protection ("OCCIP"), local FBI field offices, the FBI Internet Crime Complaint Center, or local U.S. Secret Service offices—immediately once they learn of an attack.[13] Importantly, OFAC notes that it will consider a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, made as soon as possible after discovery of an attack, to be a voluntary self-disclosure. OFAC also notes that such reports will be considered as an additional mitigating factor, and would cause OFAC to "be more likely to resolve apparent violations involving ransomware attacks with a non-public response (*i.e.*, a No Action Letter or a Cautionary Letter)[.]"[14]

d. Sanctioned Regions

Relatedly, the United States also maintains country-wide embargoes on the exportation or importation of goods, services, or technology to various countries or areas, including the Crimea region of Ukraine, Cuba, North Korea, Iran, and Syria. Many of these countries, most notably North Korea, have large cryptocurrency holdings and are reportedly using digital currencies as a means of evading existing sanctions. As a result, any transaction associated with embargoed countries should be strictly avoided, unless authorized by OFAC.

The risks associated with embargoed countries are illustrated in OFAC's February 18, 2021 settlement in the amount of approximately $500,000 with the Atlanta-based BitPay—a company that provides merchants the ability to accept digital currency as payment. As is detailed in OFAC's enforcement release, OFAC determined that BitPay potentially violated its sanctions programs over 2,000 times, when it processed crypto transactions involving its merchants' buyers, whose identification and location data (*e.g.*, IP addresses, names, phone numbers, etc.) indicated they were located in sanctioned jurisdictions.[15] No more evidence was needed for OFAC to bring an enforcement action. OFAC determined that the apparent violations occurred because BitPay failed to screen the identification and location data of the ultimate customers (the buyers) of BitPay's direct customers (the merchants).

However, OFAC gave mitigation credit to BitPay for implementing various measures to ensure against similar violations in the future, including:

- Blocking IP addresses that appear to originate in Cuba, Iran, North Korea, and Syria from connecting to the BitPay website or from viewing any instructions on how to make payment;

[13] OFAC, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments" (Sep. 21, 2021), *available online* here.

[14] *Id.* at 5.

[15] U.S. Department of the Treasury, *Enforcement Release: OFAC Enters Into $507,375 Settlement with BitPay, Inc. for Apparent Violations of Multiple Sanctions Programs Related to Digital Currency Transactions*, Feb. 18, 2021, *available online* here.

- Checking physical and email addresses of merchants' buyers when provided by the merchants to prevent completion of an invoice from the merchant if BitPay identifies a sanctioned jurisdiction address or email top-level domain; and

- Launching "BitPay ID," a new customer identification tool that is mandatory for merchants' buyers who wish to pay a BitPay invoice equal to or above $3,000. As part of BitPay ID, the merchant's customer must provide an email address, proof of identification/photo ID, and a selfie photo.[16]

These geographic restrictions present unique issues for certain coins. For example, recent reporting suggests that North Korea has invested in state-sponsored mining of Monero—a coin that has proven more difficult to trace than Bitcoin—as a means of evading existing sanctions.[17] This raises a host of difficult questions for Monero users and has almost certainly drawn the attention of OFAC. For example, if the North Korean government is mining, technically it is also validating individual transactions where its miners win the given block. U.S. persons should therefore be aware of the sanctions-related risks when undertaking any transactions involving digital currency that is validated or mined in a sanctioned jurisdiction. In turn, we must ask: would OFAC consider it a sanctions violation for a U.S. person to engage in a transaction that is validated by a miner in North Korea or another sanctioned jurisdiction? This is certainly a possible, even plain, reading of existing sanctions regulations, but the implications of that position could be catastrophic for cryptocurrencies, as it is almost certain that there are miners in embargoed countries at any given time for any given decentralized currency. Cryptocurrency users would, in effect, be rolling the dice every time they completed a transaction, hoping that a restricted miner did not randomly win the block. Similarly, U.S. miners who validate transactions for persons located in sanctioned jurisdictions also risk violating U.S. sanctions. This highlights the complexity, and potential pitfalls cryptocurrencies raise under U.S. sanctions regulations and underscores the need for further guidance from OFAC.

e. Restricted Transactions

Still more categories of sanctions pose risks for cryptocurrency transactions. OFAC also administers various less-than-comprehensive sanctions measures that do not require blocking, but instead prohibit specific transactions with sanctions targets.[18] For example, OFAC prohibits transacting in, providing financing for, or otherwise dealing in certain debt of specified tenors, or certain equity, if that debt or equity was issued by certain persons operating in Russia's financial sector. If a prohibited debt transaction is completed in cryptocurrency, U.S. persons involved in processing that transaction would be required to reject the transaction to avoid violating sanctions.

---

16 *Id.*

17 "North Korea appears to have expanded its crypto-mining operation," MIT Technology Review (Feb. 11, 2021), *available online* here.

18 Examples include the debt restrictions in the Russia/Ukraine sanctions, detailed in Directives 1-4, or the debt, securities, and equity restrictions in the Venezuelan sanctions included in Executive Orders 13808 and 13835.

This issue becomes even more complicated when one considers the possibility that the mere issuance of a coin can itself be considered a debt transaction, depending on how the coin is set up. In a now-deleted guidance statement, OFAC indicated that it would view the purchase of a digital currency produced by the Venezuelan government as an "extension of credit" to the government, in part because that currency "would carry rights to receive commodities in specified quantities at a later date."[19] OFAC specifically noted that:

A currency with these characteristics would appear to be an extension of credit to the Venezuelan government. Executive Order 13808 prohibits U.S. persons from extending or otherwise dealing in new debt with a maturity of greater than 30 days of the Government of Venezuela. U.S. persons that deal in the prospective Venezuelan digital currency may be exposed to U.S. sanctions risk. [1-19-2018][20]

When this guidance was in effect, it was highly likely that OFAC would find most uses of the government-backed currency as a violation of Executive Order 13808's restrictions on transactions involving *debt* of the Government of Venezuela with a maturity of over 30 days. Because each "token" would be deemed by OFAC an extension of credit to the Government of Venezuela, any transactions involving a token purchased from the Government of Venezuela more than 30 days prior could be deemed to "relat[e] to" the extension of illegal debt. This could be true even if the participants in the transaction were not *the original* purchasers of the token. Indeed, the token itself is potentially the debt instrument, and it could continue to mature from the moment it is first issued to the moment it is repurchased by the Venezuelan government. Although this guidance statement was removed when the Maduro regime issued the Petro, and OFAC subsequently prohibited all transactions and dealings in the Petro under Executive Order 13827, there is no evidence that OFAC has changed its views on this issue. Certain digital currencies could therefore implicate sanctions prohibitions and should be closely analyzed prior to their use.

f. Blocking and Rejecting Crypto Transactions

In general, OFAC requires U.S. persons that come into contact with a transaction involving a sanctions target to either reject the transaction (where the underlying transaction is prohibited, but there is no blockable interest) or block the transaction (where there is a blockable interest). Each requirement carries its own affirmative reporting and other obligations. For instance, OFAC regulations require U.S. persons to submit reports of rejected transactions within 10 days, including a variety of listed information about the transaction and the persons involved.[21] For any transaction that involves blocked property—*i.e.,* property owned 50% or more by an SDN—any person that holds the property must

[19] OFAC FAQ No. 551.

[20] *Id.*

[21] 31 CFR § 501.604.

continue to hold it, report the property to OFAC within 10 days, and then submit annual reports on the property thereafter.[22] Any further transfer of blocked property is itself a violation of the sanctions.

These obligations pose unique risks for cryptocurrency users. How do you reject a transaction on an exchange where the underlying mechanics of the exchange will not allow for reversing the flow of funds? How do you report required user-information if those involved are represented only by a wallet address? And for blocked funds, will exchanges be deemed to "hold" the blocked currency for the duration of the transfer? If so, primary responsibility for reporting will rest with the exchange and additional (problematic) requirements will be triggered. As one example, U.S. persons deemed to be holding blocked funds must place those funds into a "*blocked interest-bearing account*," generally defined as:

> (i) [] a federally-insured U.S. bank, thrift institution, or credit union, provided the funds are earning interest at rates that are commercially reasonable; or
>
> (ii) [] a broker or dealer registered with the Securities and Exchange Commission under the Securities Exchange Act of 1934 (15 U.S.C. 78a *et seq.*)[.][23]

These requirements will be difficult to perform for a holder of cryptocurrencies. Fortunately, OFAC has issued some helpful guidance on this front, stating that "holders" of blocked crypto assets are "not obligated to convert the blocked digital currency into traditional fiat currency (*e.g.*, U.S. dollars)."[24] In addition, it has provided examples of appropriate methods for blocking such property, stating:

Institutions may choose, for example, to block each digital currency wallet associated with the digital currency addresses that OFAC has identified as being associated with blocked persons, or opt to use its own wallet to consolidate wallets that contain the blocked digital currency (similar to an omnibus account) titled, for example, "Blocked SDN Digital Currency." Each of these methods is satisfactory, so long as there is an audit trail that will allow the digital currency to be unblocked only when the legal prohibition requiring the blocking of the digital currency ceases to apply.[25]

That said, questions remain, and well-reasoned requests to OFAC for guidance, and in some circumstances specific licenses, may be required to avoid violations and to help ensure that harmful positions are not taken by OFAC in the future.

---

[22] 31 CFR § 501.603.

[23] *E.g.* 31 CFR § 542.203 (emphasis in original).

[24] OFAC FAQ No. 646.

[25] *Id.*

g. Compliance Considerations

Given the various risks discussed above, crypto sector participants should build into their technological architecture a tailored, risk-based compliance program to identify transactions with potential sanctions exposure and prevent illicit use of their products. In some cases, it may be beneficial to engage with the Treasury Department to seek authorization or guidance regarding ambiguities in the sanctions prohibitions. Some rules may even be vulnerable to APA or other types of legal challenges in U.S. courts. Overall, although there are significant sanctions-related risks for crypto sector participants, actors in this space have many options so long as they are proactive and knowledgeable about the potential risks.

To that end, we recommend, the following basic steps (at a minimum) for U.S. participants in the cryptocurrency industry:

- Develop and implement a sanctions compliance program that incorporates each of the five core elements of compliance discussed in OFAC's Framework for OFAC Compliance Commitments:[26] (1) management commitment; (2) risk assessment; (3) internal controls; (4) testing and auditing; and (5) training;
- Screen the digital addresses, names, locations, and identifying information of all incoming and outgoing transactions. The frequency of screening will depend on the business's risk-profile, but in our view, should generally occur at account opening and periodically thereafter. It may be prudent to conduct enhanced screening of transactions involving regions in which a high concentration of SDNs are designated;
- Identify (depending on the U.S. person's risk profile) red flags that indicate that a blocked person may continue to have an interest in a digital asset, regardless of how many times the asset is transferred away from a known blocked address;
- Develop procedures to prevent transactions involving blocked coins, such as the Petro;
- Block transactions involving IP addresses, physical addresses, and other identifiers that appear to originate in sanctioned jurisdictions; and
- Consider the use of address-clustering software, where practicable, to identify addresses associated with blocked addresses that are not on the SDN List.

Overall, these basic steps can help ensure against inadvertent sanctions violations and mitigate against severe penalties should a violation nonetheless occur, though they should be tailored to the unique operations of anyone dealing in crypto currency. That said, we fully expect the compliance landscape to continue to change, as more restrictions and

[26] U.S. Department of the Treasury, *A Framework for OFAC Compliance Commitments*, May 29, 2019 *available online* here.

enforcement actions are made public. We encourage frequent reviews of any compliance program, with the assistance of experienced counsel, to ensure that you are maintaining best practices.

If you have any questions regarding this client alert, please contact the following attorneys or the Willkie attorney with whom you regularly work.

Britt Mosman
202 303 1057
bmosman@willkie.com

David Mortlock
202 303 1136
dmortlock@willkie.com

Elizabeth P. Gray
202 303 1207
egray@willkie.com

J. Christopher Giancarlo
212 728 3816
jcgiancarlo@willkie.com

Samuel Hall
202 303 1443
shall@willkie.com