20 May 2018

Client Alert: OFAC issues cryptocurrency compliance guidance, suggesting it may add digital cryptocurrency addresses to its SDN List

By Silke Elrifai

OFAC issued specific guidance on sanction compliance for transactions involving cryptocurrencies and disclosed it may include digital currency addresses on its list of Specially Designated Nationals and Blocked Persons ("SDNs"). The move is an ambitious attempt by the US government to address SDNs' increasingly sophisticated use of cryptocurrencies and other emerging payment systems to circumvent US sanctions. However, OFAC's approach is likely to accelerate the development of on-chain privacy features designed to frustrate these objectives. Moreover, cryptocurrency actors' compliance expenditures are expected to increase, especially considering President Trump's announcement on 8 May 2018 that the U.S. will re-impose far-reaching Iran sanctions.

On 19 March 2018, immediately following the issuance of President Trump's Executive Order barring any U.S.-based transactions involving Venezuela's new cryptocurrency, Petro, the Office of Foreign Asset Control ("**OFAC**") of the US Department of the Treasury issued guidance on cryptocurrencies ("**Questions on Virtual Currency**", FAQs on Sanctions Compliance Nos. 559- 563). This communication also represents a general reaction to growing concerns about malicious actors using virtual currencies to circumvent sanctions.

Those that fall under OFAC's jurisdiction must comply with its sanctions regime.

US persons are subject to OFAC jurisdiction. "US person" means any United States citizen, permanent resident alien, entity organized under the laws of the United States or any jurisdiction within the United States (including foreign branches), or any person in the United States (even if temporarily).

So-called "persons otherwise subject to OFAC jurisdiction" include, as in the case of the Cuba and Iran, non-US entities owned or controlled by US persons (*e.g.*, foreign subsidiaries) or foreign persons dealing in goods originating in the United States or containing certain levels of US content, and any person anywhere in the world causing a US person to violate US sanctions.

US persons and persons otherwise subject to OFAC jurisdiction (together "**Covered Persons**") are prohibited from engaging in trade or other transactions with SDNs or with any entity owned in the aggregate (directly or indirectly) 50 percent or more by an SDN, absent explicit OFAC exception. Covered Persons are prohibited from engaging in any unauthorized transactions, including dealings with blocked persons or property.

Fiat and cryptocurrency transactions must meet the same sanctions compliance standards.

Singling out, "firms that facilitate or engage in online commerce or process transactions using digital currency," OFAC clarified that Covered Persons are required to comply with U.S. sanctions, regardless of whether a transaction was denominated in fiat or cryptocurrency.

According to OFAC, prohibited transactions include: "dealings with blocked persons or property, or engaging in prohibited trade or investment-related transactions." Moreover, they cover transactions that evade or avoid, have the purpose of evading or avoiding, cause a violation of, or attempt to violate

prohibitions imposed by US sanctions. Significantly, persons facilitating SDNs (by providing financial, material or technological support) may risk being listed as SDNs as well.

To meet compliance requirements, OFAC mandates that: "technology companies; administrators, exchangers, and users of digital currencies; and other payment processors develop a tailored, risk-based compliance program, which generally should include sanctions list screening and other appropriate measures."

The SDN List may include a new field for digital currency addresses.

OFAC's SDN List commonly includes names of individuals, companies owned, controlled by or acting on behalf of sanctioned countries as well as individuals; and groups and entities sanctioned under non-country specific sanctions regulation, regardless of geographic location.

To strengthen its enforcement capabilities, OFAC announced that it, "may include as identifiers on the SDN List specific digital currency addresses associated with blocked persons". Defining a digital currency address as, "an alphanumeric identifier that represents a potential destination for a digital currency transfer…associated with a digital currency wallet," OFAC appears to be planning to add a new field on the SDN List for digital currency addresses and corresponding currency identifiers. For example, OFAC explicitly names bitcoin (BTC), Ether (ETH), Litecoin (LTC), Neo (NEO), Dash (DASH), Ripple (XRP), Iota (MIOTA), Monero (XMR), and Petro (PTR).

Were this new digital currency address field to be included, an individual's listing would not only include name, title, aliases, and addresses, but also associated digital addresses (*e.g.*, for illustration purposes: 1BJm2xa6csDLBukny6KGauq53Ukm6NkUcT) alongside other identifying information, such as date of birth, place of birth, nationality, passport or national identification number.

Accordingly, Covered Persons must check digital addresses against the SDN List and block or report any transactions involving those addresses. So far, the EU has not followed suit by updating its sanctions regime in a similar fashion, nor has any other country.

OFAC encourages reporting digital addresses to match already-listed individuals.

As of 17 May 2018, the SDN List did not include a digital currency address field, and it is not possible to search specifically for digital currency addresses. OFAC's guidance suggests it will update the SDN List on a rolling basis by relying on its own initiative and third-party reports to match digital addresses with already-listed SDNs.

Adding digital addresses to SDNs raises numerous questions.

How and to what extent players in the cryptocurrency space will have to adjust their operations will largely depend on whether they are considered Covered Persons and/or whether their activities could be considered prohibited transactions. For example, a multi-sig wallet provider that qualifies as a Covered Person and/or holds cryptocurrency on behalf of Covered Persons may be required to strengthen due diligence procedures significantly to ensure any cryptocurrency is not owned (directly or indirectly) 50% or more by an SDN. The compliance regimes used throughout the securities and investment sector (including investment managers and banks offering omnibus accounts) could provide a basic blueprint for cryptocurrency actors, but they may not prove sufficiently resilient in light of the risk profile of actors in the blockchain space.

OFAC has yet to provide comprehensive guidance regarding which cryptocurrency actors are Covered Persons and what checks are recommended to satisfy OFAC compliance in relation to SDNs' digital currency addresses. Thus, relevant questions remain unanswered, some of which are discussed here:

- When is a decentralized cryptocurrency actor a Covered Person?

Identifying whether a cryptocurrency actor is a Covered Person may not be straightforward in an area where decentralization is a highly-prized and frequently-claimed feature. Thus, it may be difficult to determine whether or when the creators of a decentralized autonomous organization that transacts or facilitates transactions in cryptocurrency become Covered Persons. Any determination would most likely be highly fact-based and largely dependent upon the actual governance structure.

- How extensive is the SDN tracing obligation?

Clearly, Covered Persons are prohibited from transacting with an SDN, and doing so would attract penalties. For cryptocurrency transactions where players usually put a premium on customer privacy, it may prove much more difficult to identify indirect involvement by SDNs. As such, it may be hard to identify whether the ultimate beneficial owner behind a digital address used in a transaction is majority-owned by an SDN. Various OFAC-administered sanctions regimes require Covered Persons to identify parties controlled by SDNs, which could mean identifying all users of a listed digital currency address, including for multi-sig addresses.

Doing so may prove more problematic than, for example, identifying shareholders in a company. The latter is information often readily available from company registers, or, where this is not so, available through tracing agencies specializing in uncovering the beneficial owners of shell companies.

- May digital addresses interacting with listed digital addresses become tainted by association?

It's not clear whether OFAC considers digital currency addresses that are used to send and receive coins and tokens from a SDN-listed digital currency address as tainted by association and whether those addresses would also be added to the SDN List. It is a possible outcome, given that illicit actors whose digital currency address(es) are disclosed on the SDN List would be expected to attempt to whitewash those funds by moving them quickly through a string of as-yet untainted addresses and by including non-SDNs individuals or entities.

Doing so would also significantly increase the number of blocked digital currency addresses, and include persons that should not be on the SDN List. OFAC has not indicated how many resources it plans to commit to tracing distributed ledgers to track SDNs' digital currency addresses. It's plausible that OFAC will subcontract the task to companies providing restricted party screening software. It is expected that these operations will also offer blockchain tracing services. Additionally, several start-ups are focusing on how to identify illicit activity in cryptocurrency transactions.

Difficulties would also arise if public addresses associated with third-party custodians (even unwittingly) were added to the SDN List. This action would block funds of unrelated users and/or taint their coins or tokens in the process. Moreover, the usage of tumblers and mixers may become suspect, thereby tainting the tumbled coins and tokens, short of blacklisting them.

- What are the obligations of miners?

OFAC failed to provide any details as to how it would treat node and cryptocurrency mining operators. With respect to mining, the following issues come to mind:

1. Does a mining pool become a Covered Person by having a majority of miners qualify as Covered Persons or by having the majority of servers located in the US?
2. Is mining the "facilitat[ion of]….transactions using digital currency"?
3. Must a US person that participates in a mining pool ensure that none of the other participants in the mining pool are SDNs or majority-owned by SDNs?

4. Does an administrator of a mining pool that includes US persons and SDN miners itself become a Covered Person by causing the US miner to violate US sanctions?

5. Would the mere presence of a miner, even if only indirectly controlled by an SDN, amount to a pool-wide conspiracy or attract liability for aiding and abetting or facilitation?

6. Would Covered Person miners be required to refuse to confirm transactions involving listed addresses?

Positive answers to these questions may fundamentally change mining and confirmation of new cryptocurrency transactions, greatly restricting the primary benefits of current distributed ledger technology code.

Increased digital hygiene and further exclusion of US persons are near-term consequences.

Providing answers to these questions is difficult, fact- and case-dependent, and currently involves a high level of speculation.

At this stage, it is likely that OFAC's guidance will cause actors in the cryptocurrency space to create more comprehensive compliance mechanisms. Their aim will be to exclude persons that fall within the definition of Covered Persons in order to circumvent US sanctions as much as possible. Compliance expenditures for actors in the cryptocurrency space are likely to increase, especially considering President's Trump announcement on 8 May 2018 to cease the US participation in the Joint Comprehensive Plan of Action and to re-impose the far-reaching Iran sanctions previously lifted thereunder. It will probably also involve the relocation of any remaining exchanges and other cryptocurrency actors away from US territory.

We also expect to see an increase in users' "digital hygiene," *i.e.*, the recommendation to use a digital currency address only once and for a single transaction, as well as the development of on-chain privacy features to frustrate OFAC's attempts to track SDNs' cryptocurrency associations.

Surely, however, the guidance represents a prelude to upcoming OFAC investigations into various cryptocurrency actors, and will trigger examinations by other regulators as to whether to follow suit.

If you would like more information about this topic, please contact us.

Dr. Kilian Bälz
Partner
Berlin
kb@amereller.com

Silke Elrifai
Counsel
Berlin
elrifai@amereller.com

BERLIN | Amereller Rechtsanwälte PartG mbB | Kurfürstenhöfe | Spreeufer 5 | 10178 |Berlin | Germany | t: +49.30.609.895.660