



ONPOINT / A legal update from Dechert

November 2018

OFAC Targets Digital Currency Addresses For the First Time

In a long-anticipated move, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC"), on November 28, 2018, took direct aim at the illicit use of digital currencies by identifying two digital currency addresses as associated with two Iranian individuals added to the Specially Designated Nationals and Blocked Persons ("SDN") List on the same day. As a result, digital currency transactions involving those addresses must be blocked by U.S. persons¹ because they involve the interest of an SDN. Additionally, non-U.S. persons could be subject to so-called "secondary sanctions"² for engaging in transactions involving the identified addresses.

Although the formal identification of digital currency addresses by OFAC does not alter the legal regime – U.S. persons are required to identify and block all property and interests in property in which an SDN has an interest, and to report such blocked property to OFAC – it does highlight that businesses operating in or with digital currency cannot rely upon the pseudonymous nature of such technologies to avoid OFAC compliance obligations, and especially not where OFAC has made an affirmative link between an SDN and specific digital currency addresses.

Background

In March 2018, OFAC signaled that it was actively monitoring emerging payment systems and blockchain technologies by issuing five frequently asked questions (FAQs) relating to digital currencies and sanctions compliance. In so doing, OFAC warned that it would specifically target "the use of digital currencies or other emerging payment systems to conduct proscribed financial transactions and evade U.S. sanctions" ([FAQ #561](#)).

OFAC also emphasized that the compliance obligations for U.S. persons (and for others subject to OFAC jurisdiction, such as non-U.S. entities engaging in transactions with a U.S. nexus) do not change when they are transacting or dealing in digital currencies. That is, U.S. persons, "including firms that ... process transactions in digital currency ... are responsible for ensuring that they do not engage in unauthorized transactions prohibited by OFAC sanctions, such as dealings with blocked persons or property" ([FAQ #560](#)). During the summer of 2018, OFAC underscored those obligations by reportedly issuing administrative subpoenas to various businesses operating in the digital currency space, and requesting reports of any blocked transactions or accounts and further details on internal OFAC compliance policies.

However, OFAC seemed to concede the unique challenges facing companies that operate in the digital currencies space, stating that it would consider adding "digital currency addresses to the SDN List to alert the public of specific digital currency identifiers associated with blocked persons" ([FAQ #562](#)).

The upshot of such actions is that businesses transacting or dealing in digital currencies have an ongoing obligation to ensure they are not dealing in blocked property, but that OFAC will seek to assist the private sector if and when it is able to make an affirmative link between an SDN and a digital currency address.

Designation of Iranian Cyber Actors

On November 28, 2018, OFAC made just such an affirmative link when it sanctioned two Iranian individuals, Ali Khorashadizadeh and Mohammad Ghorbaniyan, because of their alleged involvement in exchanging digital currency payments on behalf of Iranian cyber attackers involved in the SamSam ransomware scheme. OFAC went on to allege that Khorashadizadeh and Ghorbaniyan used the following two digital currency addresses to process over 7,000 transactions involving over 40 exchangers (including some U.S.-based exchangers):

- 149w62rY42aZBox8fGcmqNsXUzSStKeq8C
- 1AjZPMsnmpdK2Rv9KQNfMurTXinscVro9V

As a result, Khorashadizadeh and Ghorbaniyan were added to OFAC's SDN List, meaning U.S. persons are obligated to block and report any property in which they have an interest and that comes into a U.S. person's possession or control. As underscored by OFAC's May 2018 guidance, U.S. persons transacting or dealing in digital currencies thus have an obligation to identify and block any addresses, wallets, or transactions that they believe are owned by, or otherwise associated with, Khorashadizadeh and Ghorbaniyan, including *but not limited to* transactions that involve the addresses identified by OFAC.

OFAC also issued two new FAQs to provide guidance on how, mechanically, a U.S. person is meant to block digital currency. Much like a traditional financial institution coming into the receipt of blocked payments, OFAC advised that U.S. persons must ensure that the SDN has no access to the blocked digital currency, which can be accomplished by either:

- Blocking *each* digital currency wallet associated with the digital currency addresses identified by OFAC; or
- Creating a *new* blocked wallet to consolidate wallets that are associated with the digital currency address identified by OFAC ([FAQ #646](#)).

In either case, the blocked digital currency (like all blocked property) must be reported to OFAC within 10 days.

Takeaways

OFAC's identification of digital currency addresses that have been associated with Khorashadizadeh and Ghorbaniyan is not likely to block many transactions, due to the ease that even SDNs likely have in establishing new digital currency addresses. However, businesses transacting or dealing in digital currencies should consider the following implications:

- **The U.S. government is actively monitoring digital currency transactions.** It is unclear how OFAC and the FBI established the link between Khorashadizadeh and Ghorbaniyan and their digital currency addresses.³ However, malicious actors are now on notice that the pseudonymous nature of emerging payment systems will not shield them from potential exposure, and that the U.S. government is squarely focused on preventing the misuse of digital currencies in support of criminal activities, illicit finance, and sanctions evasion.
- **U.S. companies have an obligation to establish sanctions compliance policies.** All U.S. persons, including administrators, exchangers, and users of digital currencies, are obligated to establish "risk based" compliance policies to ensure they are not engaging in prohibited transactions with SDNs. As reflected by OFAC's issuance of administrative subpoenas to digital currency businesses, regulators will look closely at and may take enforcement action against companies who have not established and implemented robust sanctions compliance policies. At a minimum, this now means screening for digital currency addresses that OFAC has affirmatively linked to SDNs. However, U.S. persons should also have established processes in place to block and report property they have reason to believe is linked to an SDN, including digital addresses or wallets, whether or not OFAC has made such a link.
- **Non-U.S. companies face potential secondary sanctions.** Even non-U.S. persons transacting or dealing in digital currencies face potential secondary sanctions exposure if they are facilitating transactions on behalf of, or providing financial, material, or technological support for or to, SDNs. For that reason, non-U.S. administrators, exchangers, and users of digital currencies should also ensure they have OFAC screening policies in place.

Footnotes

1) U.S. persons are defined as entities organized under the laws of the United States (including foreign branches), as well as U.S. citizens and permanent residents and any persons physically present in the United States.

2) Secondary sanctions are imposed upon non-U.S. persons for engaging in specified transactions that do not have a U.S. nexus – in this case, for providing financial, material, or technological support for or to the designated SDNs –

and can result in the addition of such non-U.S. persons to the SDN List.

3) On November 28, the Department of Justice also unsealed a [criminal indictment](#) against Khorashadizadeh and Ghorbaniyan based upon the same set of facts.

This update was authored by:



Timothy Spangler
Partner, Orange County / Silicon Valley
T: +1 949 442 6044 / +1 650 813 4803
[Send email](#)



Amanda DeBusk
Partner, Washington, D.C.
T: +1 202 261 3452
[Send email](#)



Jeremy B. Zucker
Partner, Washington, D.C.
T: +1 202 261 3322
[Send email](#)



Sean Kane
Counsel, Washington, D.C.
T: +1 202 261 3407
[Send email](#)