International Trade Alert

Akin Gump
STRAUSS HAUER & FELD LLP

OFAC Adds Iranian Bitcoin Exchangers' Names and Wallet Addresses to SDN List, Ushers in "New Approach" to Sanctions Enforcement

January 10, 2019

Key Points

- On November 28, 2018, OFAC designated two Iran-based individuals who helped exchange cryptocurrency (bitcoin) into fiat currency on behalf of alleged ransomware perpetrators who targeted U.S. businesses and municipal institutions. OFAC also, for the first time, attributed specific cryptocurrency wallet addresses to these designated individuals, thereby prohibiting transactions to or from the addresses identified, among other requirements. As a result of this action, persons that transact with either SDN could be subject to sanctions.
- OFAC simultaneously released two new FAQs stating requirements and suggested methods for blocking access to, and holding, digital currency of an SDN, including creating wallet addresses specifically for consolidated holdings of blocked property.
- OFAC's attribution of specific wallet addresses to SDNs adds complexity and uncertainty to ordinary "know your customer" and sanctions diligence, since the addition of such addresses may require digital currency users to assess relationships between the published addresses and those of past or future counterparties.

Background

On November 28, 2018, the U.S. Treasury Department's Office of Foreign Assets Control (OFAC) updated its list of Specially Designated Nationals and Blocked Persons ("SDN List") with the names and, for the first time, digital currency wallet addresses, of two Iran-based individuals engaged in the exchange of bitcoin into Iranian rial on behalf of malicious cyber actors. OFAC also released two new Frequently Asked Questions (FAQ) to help U.S. financial institutions understand and comply with OFAC's requirements for blocked property as applied to digital currency. As detailed in our previous client alert, the U.S. Treasury Department's Financial Crimes Enforcement Network released an advisory last year warning financial institutions of the use by actors, such as the Government of Iran, of digital currency to circumvent U.S. sanctions. OFAC's recent action represents a concrete extension of

Contact

Wynn Segall
Partner
wsegall@akingump.com
Washington D.C.
+1 202.887.4573

Jonathan Poling
Partner
jpoling@akingump.com
Washington D.C.
+1 202.887.4029

Nnedinma Ifudu Nweke
Partner
nifudu@akingump.com
Washington D.C.
+1 202.887.4013

Jung Hwa Song
Associate
jsong@akingump.com
New York
+1 212.872.8020

Chris Chamberlain
Associate
cchamberlain@akingump.com
Washington D.C.
+1 202.887.4308

Michael Adame
Law Clerk
madame@akingump.com
Washington D.C.
+1 202.419.4627

this general warning, and a senior OFAC official recently heralded the designations and wallet associations as a "new approach" to sanctions enforcement in the context of digital currency and related networks.

OFAC Designates Iran-Based Bitcoin Exchangers and Publishes Associated Addresses

OFAC designated the two Iran-based individuals pursuant to Executive Order 13694, as amended, for providing support to individuals involved in certain cyber-enabled attacks employing the so-called SamSam ransomware against a variety of U.S. public and municipal institutions. According to OFAC's press release, Ali Khorashadizadeh and Mohammad Ghorbaniyan facilitated the exchange of bitcoin derived from the SamSam ransomware attacks into Iranian rial, including by depositing the rial into Iranian banks. OFAC alleged that, since 2013, the two individuals used the two specified wallets to process more than 7,000 bitcoin transactions with more than 40 exchangers, including some based in the United States, and sent approximately 6,000 bitcoins worth millions of U.S. dollars, some of which derived from the SamSam ransomware activity. Importantly, OFAC's press release does not suggest that Khorashadizadeh and Ghorbaniyan were directly involved, or even aware of, the related ransomware activities or aware of the illicit source of the digital assets.

New FAQs Outline Requirements and Methods for Blocking Digital Currencies

Concurrently with its designations, OFAC released two new FAQs reiterating the requirement to block the property of SDNs and proposing potential methods for holding blocked digital currency. For example, OFAC explains in FAQ 646 that "[i]nstitutions may choose . . . 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.'" OFAC notes that either method would be satisfactory "so long as there is an audit trail" to permit the digital currency to be unblocked in the future.

The FAQs also explain that, while holding the blocked currency, the financial institution is not obligated to convert it into a traditional fiat currency (e.g., U.S. dollars). The financial institution must, however, report to OFAC that it is holding blocked digital currency within 10 business days. Finally, OFAC notes in FAQ 647 that a financial institution may notify a customer that it has blocked the customer's digital currency and that the customer has the right to apply for the unblocking and release of the digital currency through ordinary release procedures.

Observations and Recommendations

- OFAC's actions are broadly significant because they demonstrate OFAC's increasingly aggressive approach to sanctions enforcement, namely the pursuit (and designation) of digital currency exchangers and other service providers, irrespective of their involvement in, or knowledge of, the malicious, cyber-enabled activities underlying the designations.

- OFAC's attribution of digital wallet addresses is also significant because it adds a layer of complexity and uncertainty for sanctions diligence by both exchangers and individual users of digital currencies. While OFAC did not specify how it expects industry to use the named addresses or what due diligence activities might warrant mitigation, OFAC indicated its view that the published addresses "should assist those in the compliance and digital currency communities in identifying transactions and funds that must be blocked and investigating any connections to these addresses." OFAC did not explain what degree of proximity or separation would amount to a problematic "connection[]" to a specified wallet address. At a minimum, we recommend that companies identify and analyze any correlations and transactions involving the published addresses and those of future (or past) counterparty addresses to facilitate an assessment of sanctions risk.
- With respect to enforcement, OFAC's actions may preview forthcoming enforcement actions against U.S. persons for transacting with, or holding the digital currency of, the SDNs, the associated wallet addresses, or other persons and addresses connected to them. The designations also bring the Treasury's wider approach to Iranian sanctions into focus and highlight the high stakes and level of care required when transacting with individuals or entities with any nexus to Iran, particularly when doing so using digital currencies.