PAUL HASTINGS

STAY CURRENT

November 2018

Follow @Paul_Hastings

The Blocking of Digital Currency: A New Phase of Sanctions Enforcement

By Behnam Dayanim, Dina Ellis Rochkind, Lara Kaplan & Talya R. Hutchison

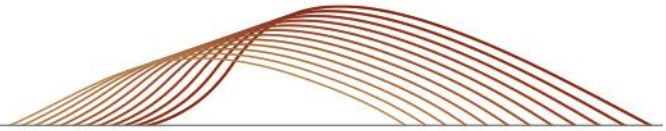
On November 28, 2018, the U.S. Department of the Treasury's Office of Foreign Assets Control ("OFAC") for the first time published the digital currency addresses associated with specific individuals subject to sanctions. OFAC, the primary agency in charge of administering U.S. economic sanctions programs, has the authority to block property of persons involved in "malicious cyber-enabled activities" originating from outside of the United States and who constitute a threat to national security or the financial stability of the United States.[1] They have now used that authority in a new way: blocking specific digital currency addresses associated with two persons who assisted in a cyberattack.

Aiding in a Ransomware Attack

Since 2015, a cyberattack conducted with SamSam ransomware has targeted over 200 known victims, costing them collectively more than $30 million. The Iranian-based perpetrators, now reportedly indicted by the Department of Justice, used the ransomware to gain administrator rights to networks and hold the networks hostage until a ransom was paid. They instructed that ransom be paid in bitcoin, and two men, Ali Khorashadizadeh and Mohammad Ghorbaniyan, helped facilitate this payment.

According to the Treasury Department, Mr. Khorashadizadeh and Mr. Ghorbaniyan facilitated the digital currency ransom payments by exchanging the digital currency into Iranian rial on behalf of the perpetrators of the attacks and then depositing the currency into the Iranian financial system.[2] Over 7,000 transactions in bitcoin were processed through two digital currency addresses associated with Mr. Khorashadizadeh and Mr. Ghorbaniyan. These transactions involved over 40 exchangers and involved the transfer of approximately 6,000 bitcoins.

Mr. Khorashadizadeh and Mr. Ghorbaniyan are now considered to be Specially Designated Nationals ("SDNs"), effectively prohibiting U.S. persons from transacting with them. In its press statement announcing the designations, OFAC also brandished the threat of potential "secondary sanctions"—penalties against non-U.S. persons for doing business with either man, although the agency did not elaborate. In an unprecedented move, however, OFAC did not just list traditional identifiers on Mr. Khorashadizadeh and Mr. Ghorbaniyan's SDN entries (such as date of birth or address); OFAC has also listed their associated digital currency addresses. The program under which Mr. Khorashadizadeh and Mr. Ghorbaniyan were sanctioned requires all property in which either man has an interest and that is either held by a U.S. person or is located within the United States to be "blocked."



"Blocking" means prohibiting the transfer, withdrawal, or other disposition of the property and reporting that is being held to OFAC. Because the digital currency addresses were included in the listing, transactions involving those addresses will be considered transactions with the individuals themselves, and any funds connected to those addresses must be blocked.[3]

Blocking of Digital Currency Addresses

A digital currency address is a string of letters and numbers that acts as a potential destination for a digital currency transfer. (Bitcoin is a well-known digital currency, but there are thousands of such currencies in existence.) The address often relates to an open source software program, a digital currency wallet, which is used to generate and store digital currency addresses as well as maintain digital currency balances. An address is needed in order to engage in digital currency transactions and acts as a mechanism to send and receive digital assets.

In its action against Mr. Khorashadizadeh and Mr. Ghorbaniyan, OFAC published the two digital currency addresses associated with each of them that were used to process the bitcoin ransom transactions. These addresses now comprise part of Mr. Khorashadizadeh and Mr. Ghorbaniyan's SDN List entry. Therefore, funds related to those digital currency addresses are considered to be blocked property.

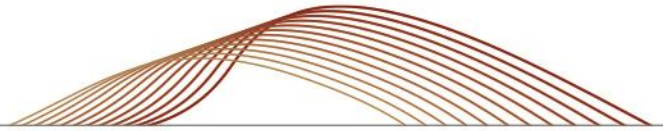
As this issuance of sanctions marks the first time that a digital currency address has been designated as associated with an SDN, and therefore considered blocked property, OFAC has issued guidance regarding how to block such transactions.[4] When an institution discovers it is in possession of digital currency required to be blocked, the institution must block access to the digital currency. It may do so by blocking the individual digital currency wallet or it may consolidate all blocked wallets into an institutional wallet designed to hold the blocked digital currency. Though institutions are not required to transfer the digital currency into fiat currency, the institution must ensure that the digital currency may only be unblocked when it is legally permissible to do so. OFAC also requires that blocked digital currency must be reported within 10 business days.

A New Phase of Sanctions

This step, if successful, will have ramifications for all sanctions programs, but particularly Iran. Iranian hackers have increasingly used ransomware attacks paired with digital currency ransom payments over the past several years.[5] By including the digital currency address along with an individual listing, OFAC is hoping to choke off what it sees as an increasingly utilized method for perceived bad actors to evade U.S. sanctions.

For more information or to discuss how best to comply with these new requirements, please contact any member of our National Security Regulation and Investigations Practice.

✧ ✧ ✧



If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings Washington, D.C. lawyers:

Behnam Dayanim
1.202.551.1737
bdayanim@paulhastings.com

Robert P. Silvers
1.202.551.1216
robertsilvers@paulhastings.com

Talya Hutchison
1.202.551.1930
talyahutchison@paulhastings.com

Scott M. Flicker
1.202.551.1726
scottflicker@paulhastings.com

Dina Ellis Rochkind
1.202.551.1938
dinaellis@paulhastings.com

Lara Kaplan
1.202.551.1868
larakaplan@paulhastings.com

Lawrence D. Kaplan
1.202.551.1829
lawrencekaplan@paulhastings.com

---

[1] Exec. Order No. 13,694, 80 Fed. Reg. 18,077 (Apr. 1, 2015).

[2] Press Release, U.S. Dep't Treasury, Treasury Designates Iran-Based Financial Facilitators of Malicious Cyber Activity and for the First Time Identifies Associated Digital Currency Addresses (Nov. 28, 2018), https://home.treasury.gov/news/press-releases/sm556.

[3] *Id*.

[4] Questions on Virtual Currency, OFAC Resource Center (Nov. 28, 2018), https://www.treasury.gov/resource-center/faqs/Sanctions/Pages/faq_compliance.aspx#646.

[5] Robert McMillan, *Iranian Hackers Turn to Ransomware, Bitcoin as Economy Stalls*, WALL ST. J. (Aug. 7, 2018), https://www.wsj.com/articles/iranian-hackers-turn-to-ransomware-bitcoin-as-economy-stalls-1533671703.