Cleary Foreign Investment and International Trade Watch

OFAC Updates Ransomware Advisory and Sanctions Virtual Currency Exchange

By Chase D. Kaniecki, Samuel H. Chang & Megan Lindgren on September 27, 2021

On September 21, 2021, the U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC): (i) issued an **updated advisory** on potential sanctions risks for facilitating ransomware payments; and (ii) designated SUEX OTC, S.R.O. (SUEX), a virtual currency exchange, on the list of Specially Designated Nationals and Blocked Persons (SDN List) for its role in facilitating financial transactions for ransomware actors.[1] These actions demonstrate the U.S. government's increasing focus on virtual currencies as a key means of facilitating ransomware payments and related money laundering, as well as OFAC's commitment to combating ransomware attacks and other malicious cyber activities.

Updated OFAC Advisory

As explained in our earlier **blog post**, OFAC previously published an **advisory** regarding cyber ransom payments that described how U.S. economic sanctions apply to ransomware payments and offered guidance on its compliance expectations and enforcement considerations.[2]

OFAC's latest advisory, which updates the prior advisory, makes it clear that the U.S. government "strongly discourages" payment of cyber ransoms (it previously said that it "does not encourage" paying ransoms but "understands" that it may occur). In addition, the advisory highlights two "significant mitigating factors" in determining whether to pursue an enforcement action and the amount of any penalty for sanctions violations relating to ransomware payments:

- Attack Prevention Measures. OFAC will consider the strength of a company's cybersecurity protections and referenced **CISA's Ransomware Guide** as guidance, including whether a company maintains offline backups of data, develops incident response plans, institutes cybersecurity training, regularly updates antivirus and anti-malware software, and employs authentication protocols.[3]
- Reporting. OFAC will consider a company's outreach to the U.S. government (including the Cybersecurity and Infrastructure Security Agency (CISA), the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), or law enforcement) "as soon as possible after discovery of an attack" and ongoing cooperation to provide all relevant information, such as technical details, ransom payment demand, and ransom payment instructions, in evaluating whether or not to pursue an enforcement action if the payment involved a sanctions violation. Notably, such reporting could be considered a voluntary self-disclosure, which would reduce the base penalty for any sanctions violations associated with the payment by as much as 50%.

OFAC also stated that such mitigating steps—and self-reporting in particular—would increase the likelihood that any violation would be resolved with a non-public response such as a No Action Letter or a Cautionary Letter.

Designation of SUEX

In addition, for the first time, OFAC **designated** a virtual currency exchange, SUEX, on the SDN List pursuant to **Executive Order 13694** for providing material support to ransomware actors.[4] SUEX has been reported to be a Czech-registered and Russian-owned company that engages extensively with illicit actors. According to OFAC, over 40% of the exchange's known transaction history was associated with illicit actors.

SUEX operates as a "nested" exchange, in which it accepts customers upon referral by intermediaries and provides an interface for customers to trade virtual currencies through larger exchanges. As a result of the designation, all property and interests in property of SUEX (as well as entities 50% or more owned by SUEX) that are subject to U.S. jurisdiction are blocked, and U.S. persons, including U.S. financial institutions and intermediaries, are prohibited from engaging in transactions or dealings with or involving SUEX (as well as entities 50% or more owned by SUEX). Also, non-U.S. persons,

including non-U.S. financial institutions, face secondary sanctions risk if they provide material assistance or support to SUEX.

In light of the above, companies, particularly those in the virtual currency space, should consider implementing or enhancing existing due diligence procedures to ensure that none of the parties involved in a particular transaction are sanctioned. In so doing, parties should pay particular attention to peer-to-peer exchangers, mixers, tumblers, and similar services known to facilitate illicit transactions. In addition, U.S. persons with hosted wallets held by third parties in particular should consider the risk of future restrictions on their assets in the event that the entity offering custodial services is designated. Going forward, as U.S. authorities receive more detailed information from reporting of ransomware attacks, companies should be prepared for additional designations and enforcement actions by OFAC against actors in the virtual currency industry.

---

[1] *See* Press Release, U.S. Department of the Treasury, "Treasury Takes Robust Actions to Counter Ransomware" (Sept. 21, 2021), **https://home.treasury.gov/news/press-releases/jy0364**.

[2] *See* Press Release, U.S. Dep't of the Treasury, "Treasury Department Issues Ransomware Advisories to Increase Awareness and Thwart Attacks" (Oct. 1, 2020), **https://home.treasury.gov/news/press-releases/sm1142**.

[3] *See* Cybersecurity & Infrastructure Security Agency, Ransomware Guide (Sept. 2020), **https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf**.

[4] U.S. Department of the Treasury, "Publication of Updated Ransomware Advisory; Cyber-related Designation" (Sept. 21, 2021), **https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20210921**.

Cleary Foreign Investment and International Trade **Watch**