SULLIVAN & CROMWELL LLP

S&C memo

September 23, 2021

OFAC Updates Ransomware Advisory

New Guidance Incentivizes Reporting, Defensive Cybersecurity Measures for Companies Facing Ransomware Attacks

SUMMARY

On September 21, 2021, the United States Department of the Treasury's Office of Foreign Assets Control issued an *Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments,* which provides additional guidance for companies facing ransomware attacks, or processing ransomware payments, on ways to mitigate the risks of a potential sanctions violation in connection with such payments. The Updated Advisory incentivizes companies to proactively improve their information security systems and to promptly report ransomware attacks to U.S. government agencies by offering penalty mitigation under OFAC's enforcement guidelines in the event a sanctions violation is later discovered. Concurrent with the release of the Updated Advisory, OFAC issued the first designation of a virtual currency exchange under Executive Order 13694 for providing material support to the threat posed by criminal ransomware actors.

BACKGROUND

The Office of Foreign Assets Control ("OFAC") first published a ransomware advisory on October 1, 2020 (the "October 2020 Advisory") explaining Treasury's views on potential sanctions risks involved in ransomware payments. Among other things, OFAC highlighted the risk that a victim might only discover after the fact that a ransomware payment involved a sanctioned actor or jurisdiction and thus constituted a potential violation of U.S. sanctions. For additional background on the October 2020 Advisory and the intersection of ransomware and U.S. sanctions, see S&C's client publication and the corresponding episode of *S&C Critical Insights* on the subject.

A. UPDATED ADVISORY

Unlike the October 2020 Advisory, which did not set forth an official position on the payment of ransoms, the September 21, 2021 update (the "September 2021 Advisory") states "[t]he U.S. government strongly discourages all private companies and citizens from paying ransom or extortion demands." Furthermore, the September 2021 Advisory articulates mitigating factors under OFAC's Enforcement Guidelines[1] that OFAC will consider if a company has paid or facilitated a ransom that is ultimately determined to have violated sanctions. Specifically, OFAC will consider whether the victim company had instituted appropriate cybersecurity measures prior to the attack, whether the attack was promptly reported to the U.S. government and law enforcement, and whether there was meaningful cooperation with law enforcement and the U.S. government.

1. Defensive Cybersecurity Measures

According to the September 2021 Advisory, "meaningful steps to reduce the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices . . . will be considered a significant mitigating factor in any OFAC enforcement response." Measures described in the advisory include:

- Maintaining offline backups of data;
- Developing incident response plans;
- Instituting cybersecurity training;
- Regularly updating antivirus and anti-malware software; and
- Employing authentication protocols.

For additional cybersecurity best practices, OFAC advises companies to consult the Cybersecurity and Infrastructure Security Agency ("CISA") September 2020 Ransomware Guide.[2]

2. Cooperation with OFAC and Law Enforcement

The September 2021 Advisory states that OFAC is more likely to resolve potential enforcement cases involving ransomware with a non-public No Action Letter or Cautionary Letter when the victim took mitigating steps "particularly reporting the ransomware attack to law enforcement as soon as possible and providing ongoing cooperation." Other factors that OFAC views as mitigating include the nature and extent of cooperation with OFAC, law enforcement, and other relevant agencies, as well as whether the apparent violation of U.S. sanctions is voluntarily self-disclosed. The September 2021 Advisory also clarifies that disclosures to U.S. government agencies other than OFAC, made as soon as possible after an attack, are considered by OFAC to be a voluntary self-disclosure, even if a potential sanctions nexus is not discovered until later, although OFAC should be notified once such a nexus is identified by the victim. In addition to reporting, examples of cooperation include the provision by the victim of technical details related to an attack, ransom payment demand information, and ransom payment instructions.

B. DESIGNATION OF SUEX

Concurrent with the release of the September 2021 Advisory, OFAC designated Suex OTC, S.R.O. ("Suex"), a nested virtual currency exchange[3] with physical locations in Russia and the Czech Republic, pursuant to Executive Order 13694, as amended by Executive Order 13757.[4] The Suex designation—the first of a virtual currency exchange—was issued as a result of the exchange's facilitation of financial transactions on behalf of ransomware actors. According to OFAC, over 40% of known Suex transactions involved illicit actors and the exchange facilitated transactions involving at least eight ransomware variants. Reporting suggests that Suex dealt with clients exclusively via encrypted messaging applications and only accepted new clients via referrals from trusted intermediaries.[5]

IMPLICATIONS

The September 2021 Advisory is the latest step in the Biden administration's efforts to address the nation's cybersecurity. Those efforts began with the May 12, 2021 Executive Order on Improving the Nation's Cybersecurity[6] and include the July 28, 2021 National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems,[7] as well as meetings with industry leaders across the United States.[8] The September 2021 Advisory underscores the seriousness of the threat posed by ransomware and makes clear that cybersecurity is a top priority for the nation that requires a whole-of-nation approach. The September 2021 Advisory also follows high-profile attacks on critical infrastructure, including the May 2021 attack on Colonial Pipeline, which disrupted nearly half of the East Coast's delivery of diesel, gasoline, and jet fuel.

The September 2021 Advisory incentivizes companies to prepare for the possibility of attacks, and cooperate fully with the U.S. government in the event such an attack occurs, in order to limit the risk and severity of a follow-on enforcement action. By offering mitigation credit and a non-public enforcement response to companies that are proactive in improving their cybersecurity policies, processes, and infrastructure; are proactive in reporting attacks; and offer meaningful cooperation to the U.S. government, the Biden administration aims to push companies into adopting better cybersecurity practices without a formal mandate. Companies should consider the guidance in the September 2021 Advisory and the potential benefits it offers as they design and implement their cybersecurity programs.

The Suex designation is notable in that it represents the first designation of a virtual currency exchange, rather than an individual ransomware perpetrator or associated virtual currency wallet. The Biden administration has taken action against the financial facilitators of ransomware attacks as part of an effort to disrupt the larger virtual currency ecosystem that enables the perpetrators of ransomware attacks. This action—along with earlier FinCEN and DOJ actions targeting virtual currency exchange BTC-e and virtual currency mixer Helix—represents a warning to virtual currency exchanges that fail, either knowingly or inadvertently, to ensure that their platforms are not used to facilitate ransomware payments. Treasury officials have signaled that the Suex designation may represent a first step in a broader campaign. As

Deputy Secretary Adeyemo stated to reporters, "Treasury will prioritize the identification of nested exchanges transacting high percentages of illicit activity."[9]

* * *

---

1 *See* 31 C.F.R. Part 501, App. A.

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

3 A nested virtual currency exchange operates by opening accounts with one or more other exchanges in its own name and conducting trades without disclosing the identity of its underlying clients. *See, e.g.*, CHAINALYSIS, *270 Service Deposit Addresses Drive 55% of Money Laundering in Cryptocurrency* (Feb. 11, 2021), https://blog.chainalysis.com/reports/cryptocurrency-money-laundering-2021.

4 Exec. Order 13694, 80 Fed. Reg. 18077 (Apr. 1, 2015); Exec. Order 13757, 82 Fed. Reg. 1 (Dec. 28, 2016).

5 TRM Labs, "Behind Suex.io: the first sanctioned cryptocurrency exchange" (Sept. 21, 2021), https://www.trmlabs.com/post/behind-suex-io-the-first-sanctioned-cryptocurrency-exchange.

6 Exec. Order 14028, 86 Fed Reg. 26633 (May 17, 2021). For further details, please see our client publication on this Executive Order.

7 NSM–5: Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (July 28, 2021).

8 *See* Fact Sheet: Biden Administration and Private Sector Leaders Announce Ambitious Initiatives to Bolster the Nation's Cybersecurity (Aug. 25, 2021), https://www.whitehouse.gov/briefing-room/statements-releases/2021/08/25/fact-sheet-biden-administration-and-private-sector-leaders-announce-ambitious-initiatives-to-bolster-the-nations-cybersecurity/.

9 Ian Talley and Dustin Volz, "U.S. Sanctions Crypto Exchange Accused of Catering to Ransomware Criminals," *WSJ* (Sept. 21, 2021), https://www.wsj.com/articles/u-s-treasury-threatens-more-sanctions-targeting-crypto-services-found-aiding-illicit-actors-11632234624?mod=djemRiskCompliance; Nicole Sganga, "Biden administration sanctions virtual currency exchange following spike in ransomware attacks," *CBS News* (Sept. 21, 2021), https://www.trmlabs.com/post/behind-suex-io-the-first-sanctioned-cryptocurrency-exchange.

ABOUT SULLIVAN & CROMWELL LLP

Sullivan & Cromwell LLP is a global law firm that advises on major domestic and cross-border M&A, finance, corporate and real estate transactions, significant litigation and corporate investigations, and complex restructuring, regulatory, tax and estate planning matters. Founded in 1879, Sullivan & Cromwell LLP has more than 875 lawyers on four continents, with four offices in the United States, including its headquarters in New York, four offices in Europe, two in Australia and three in Asia.

CONTACTING SULLIVAN & CROMWELL LLP

This publication is provided by Sullivan & Cromwell LLP as a service to clients and colleagues. The information contained in this publication should not be construed as legal advice. Questions regarding the matters discussed in this publication may be directed to any of our lawyers or to any Sullivan & Cromwell LLP lawyer with whom you have consulted in the past on similar matters. If you have not received this publication directly from us, you may obtain a copy of any past or future publications by sending an e-mail to SCPublications@sullcrom.com.