PAUL HASTINGS

Stay Current

September 2021

Follow @Paul_Hastings

Unprecedented Sanctions on Crypto Exchange Signal New Strategy against Ransomware Threats

By Kenneth M. Breen, Phara Serle Guberman & Liam Murphy

In an unprecedented action on September 21, 2021, the Department of Treasury ("Treasury") blacklisted a Russian-based cryptocurrency exchange SUEX OCT, S.R.O. ("SUEX"), for allegedly facilitating transactions on behalf of ransomware actors and other cybercriminals. The Treasury's Office of Foreign Assets Control ("OFAC") designated SUEX as a "malicious cyber actor" and added it to the "Specially Designated Nationals" list, a list of individuals and companies allegedly owned or controlled by, or acting for or on behalf of, targeted countries, terrorist organizations, or narcotics traffickers.[1] As a result, any U.S. company or entity is generally prohibited from transacting with SUEX, and any SUEX property or interests in property that are in the U.S. (or later come into the U.S.) may not be transferred or otherwise withdrawn.[2] Since the designation, other cryptocurrency exchanges have announced that they are barring transactions with accounts that had dealt with SUEX.

This is the first instance of the U.S. government imposing sanctions on a cryptocurrency exchange for its purported participation in cybercriminal activity, indicating a new focus on investigating and potentially bringing sanctions against the wider cryptocurrency network to address increasing ransomware attacks. The Treasury concurrently provided updated guidance on best practices for the private sector to prepare for and respond to ransomware attacks, emphasizing increased proactive cybersecurity efforts, prompt reporting of cyberattacks, and sanctions risks for failed cybersecurity compliance. The sanctions against SUEX raise questions about private sector liability after a crypto attack, including whether ransomware victims and third-party intermediaries (e.g., insurance companies) can in some circumstances face liability if they pay ransoms.

Ransomware Guidance Provides Mitigation Steps to Combat Cyberattacks and Reiterates Warnings Concerning Ransomware Payments

Ransomware is a type of malicious software that threatens to publish or block access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker. Ransomware attacks are increasing exponentially as technology improves. In 2020, ransomware payments reached over $400 million, more than four times the level in 2019. In the press release announcing sanctions on SUEX, Treasury Secretary Janet Yellen stated, "[a]s cyber criminals use increasingly sophisticated methods and technology, we are committed to using the full range of measures to include sanctions and regulatory tools, to disrupt, deter, and prevent ransomware attacks."

In tandem with the sanctions, OFAC issued guidance on how the private sector should respond to ransomware attacks. The guidance stressed the importance of companies implementing cybersecurity practices to reduce the risk of extortion, including maintaining offline backups of data, developing incident response plans, instituting cybersecurity training, regularly updating antivirus and anti-malware software, and employing authentication protocols. Additionally, the updated advisory states that OFAC "strongly encourages all victims and those involved with addressing ransomware attacks to report the incident" as soon as possible.

The recent guidance also reiterated the U.S. government's warnings concerning the payment of ransoms or otherwise complying with their extortion demands. Last year, OFAC issued a pair of similar advisories. Those advisories specifically called out intermediaries that negotiate with hackers on behalf of cyberattack victims, including insurance companies that cover ransomware payouts as part of cyberattack insurance policies, and advised that such payouts could be in violation of the law if they are found to have "facilitated" the transfer of funds to a designated entity.

If a company is the subject of a cyberattack and pays the ransom to a designated entity, OFAC's recent guidance now considers that company's cybersecurity policies, procedures, and implementation, as well as the prompt reporting of the attack to law enforcement, as mitigating factors when it considers assessing penalties.

Conclusion

The blacklisting of SUEX, and the related Treasury guidance, signals the U.S. government's strategy to involve the private sector in combating cybercriminal activity. The designation of SUEX as a "malicious cyber actor" creates a precedent for future designations of other cryptocurrency exchanges and others for facilitating payments to cybercriminal actors, or otherwise acting without appropriate compliance measures to thwart or identify such activity.

Private sector companies and third-party intermediaries must also take notice. Ransomware attacks are becoming more common, increasingly threatening companies and their data. Companies should regularly assess and test their cyber policies and procedures, ensuring robust and effective controls are in place. Entities should also be prepared to promptly disclose ransomware threats and preventive actions taken (including the paying of a ransom) in order to mitigate the risk of sanctions following an attack.

✧ ✧ ✧

If you have any questions concerning these developing issues, please do not hesitate to contact any of the following Paul Hastings New York lawyers:

Kenneth M. Breen
1.212.318.6344
kennethbreen@paulhastings.com

Phara Serle Guberman
1.212.318.6252
pharaguberman@paulhastings.com

Liam Murphy
1.212.318.6713
liammurphy@paulhastings.com

[1] Executive Order 13694: Blocking the Property of Certain Persons Engaging in Significant Malicious Cyber-Enabled Activities (Apr. 1, 2015).

[2] *Id.*