LAW360

Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Crypto Exchange Blacklisting To Test US Sanctions' Teeth

By **Ben Kochman**

Law360 (September 24, 2021, 6:30 PM EDT) -- The U.S. Department of the Treasury's unprecedented blacklisting of a cryptocurrency platform accused of helping cybercriminals convert funds into real-world currency will test its ability to sway ransomware actors' behavior, as officials sharpen their pitch for victims to report attacks.

Treasury's move on Tuesday to add Russia-based SUEX to the government's sanctions list — the agency's first labeling of a cryptocurrency exchange as a "malicious cyber actor" — also signals authorities' strategy to focus their sanctions efforts, at least at first, on the wider ecosystem that enables attacks rather than on attackers themselves.

Targeting a cryptocurrency exchange rather than a ransomware cartel with sanctions serves at least two purposes, ex-government officials tell Law360. First, going after exchanges allows U.S. officials to target a platform used by several ransomware gangs at once, with the aim of cutting them off from tools they have used to launder extortion funds into cash or other assets.

The move also shows sensitivity to private-sector concerns that ransomware victims and third-party intermediaries like insurance companies and forensic firms could face liability if they pay ransoms to groups that are determined at any point to be subject to U.S sanctions.

"Targeting the ransomware groups themselves would be a potential step, but would also create an obvious problem for many victims in that they would be unable to pay [without facing legal risks]," said Brandon Van Grack, a partner at Morrison & Foerster LLP who spent more than a decade at the U.S. Department of Justice, including as chief of the Foreign Agents Registration Act unit.

"It appears that the government wants to aggressively tackle this issue, but in a way that shows that they are understanding of the challenges that victim companies face," said Van Grack, who added, "This was not the most aggressive sanctions action that we could have seen."

Despite the FBI's advice that paying ransoms will embolden future attacks, many victims continue to pay them. According to Treasury Department statistics, cybercriminals received more than $400 million in ransomware payments in 2020, more than four times the amount paid in 2019.

Determining which members of which ransomware crews to sanction is also challenging as the gangs play cat-and-mouse games with authorities, industry attorneys say. The Russia-based "DarkSide" crew accused of carrying out this year's headline-grabbing ransomware attack on Colonial Pipeline Co., for

example, claimed to have disbanded soon after the attack.

But a new cybercriminal crew calling itself "BlackMatter" has appeared in recent weeks and bears several similarities to the DarkSide group, cybersecurity experts say.

"Cybercriminal groups are constantly engaging in rebranding, and it's very difficult to trace who the criminals are behind specific groups, but when you are dealing with an exchange, you are attempting to stop a facilitator of the attacks," said William Ridgway, a partner in the privacy and cybersecurity practice at Skadden Arps Slate Meagher & Flom LLP and former federal prosecutor. "I can see why this may be an effective use of government resources."

It remains to be seen to what extent Treasury's sanctions targeting SUEX will slow or shut off the flow of money to the company, which has received more than $160 million in bitcoin from ransomware actors and other cybercriminals since 2018, according to Chainalysis, a company that analyzes cryptocurrency transactions.

But an announcement on Wednesday that Binance, the world's largest cryptocurrency exchange, had barred transactions with "several" accounts that had dealt with SUEX is a sign that added attention on the company could affect its operations.

In a blog post, Binance CEO Changpeng Zhao wrote that Binance had revoked access to the accounts based on its own internal safeguards earlier this year.

The company added that it had shared information about the 25 blockchain addresses blacklisted by the Treasury Department on Tuesday with the "appropriate authorities," and that it would continue working with law enforcement "to cast sunlight on those threat actors that seek to abuse our platforms," like SUEX.

"SUEX relies on the infrastructure of established cryptocurrency exchanges to conduct its transactions — exchanges that are now prohibited from dealing with SUEX," said Alex Iftimie, a Morrison & Foerster partner and a former DOJ national security official from 2012 to 2019.

Iftimie called Tuesday's sanctions "a bellwether for whether U.S. sanctions are effective against cryptocurrency exchanges," adding that if authorities are "successful in disrupting SUEX's and similar exchanges' operations, it will force criminals to platforms that are easier for law enforcement to track."

Officials from Treasury's Office of Foreign Assets Control, or OFAC, also reiterated their call Tuesday for ransomware victims to tell law enforcement about attacks. The agency listed new details on what the government would consider a "significant mitigating factor" in bringing an enforcement action against a company that facilitates a ransomware payment to a sanctioned actor, including revealing technical details about the attack and information on the amount of ransom demanded.

For the first time, OFAC said it would also consider it a mitigating factor if an attack victim had followed the U.S. Cybersecurity and Infrastructure Security Agency's suggestions for avoiding being hit, including maintaining offline backups of data and training employees about cybersecurity threats.

"OFAC is trying to come up with positive incentives for companies to take proactive efforts here, and I think that shows that they are being more reasonable about understanding the difficult situation that ransomware victims are in," said Guillermo Christensen, a partner in the data security and privacy group

at Ice Miller LLP and a former CIA intelligence officer.

More visibility of ransomware attacks as they happen is likely to lead to more sanctions against actors in the ransomware ecosystem down the road, ex-government officials say.

"The guidance increasingly puts pressure on companies to provide more details about where the ransomware funds are being directed, which could create a feedback loop in which Treasury uses that information to issue further sanctions against actors in this space," said Skadden's Ridgway.

--Editing by Philip Shea and Kelly Duncan.
