FiveBy

ADVISORY

OFAC Sanctions First Cryptocurrency Exchange, Extra Due Diligence Needed

This week the US Treasury's Office of Foreign Assets Control (OFAC) sanctioned cryptocurrency exchange SUEX OTC that allowed ransomware operators and other illicit actors to instantly transfer the proceeds of criminal activity, highlighting the US government's promise to increase focus on ransomware. Analysis of known SUEX transactions shows that more than 40 percent of the company's known transaction history is associated with illicit actors. FiveBy judges that this is only the first of numerous exchanges and virtual currency mixers that OFAC will target in an effort to disrupt the scourge of ransomware. Therefore, US firms and financial institutions will need to enhance their due diligence, know-your-customer, and sanctions compliance programs to avoid risk associated with these government efforts.

- In June, after a ransomware attack against the Colonial Pipeline by a suspected Russian ransomware group known as DarkSide wreaked havoc with gas prices and caused localized fuel shortages, the Justice Department implemented a specialized process similar to counterterrorism efforts undertaken after the September 11th attacks to counter ransomware and other digital crimes. The White House this year also engaged with foreign partners and allies to hold ransomware perpetrators accountable.

- OFAC has updated an advisory issued last year on the potential sanctions risks for facilitating ransomware payments providing information on and highlighting the importance of cooperating with the US government in the event of a ransomware attack.

- SUEX is a nested exchange that is registered in Czechia but based in Russia, which uses accounts at major global cryptocurrency exchanges to provide services to its clients and allow them to conduct virtual currency transactions. The concept is similar to nested accounts—foreign bank accounts that are lodged within other foreign bank accounts and tied to a corresponding US account—which have long been flagged as a money-laundering risk.

Although screening against sanctions lists to avoid doing business with possible individuals or entities on OFAC's specially designated nationals and blocked persons (SDN) list is important, companies can do more to protect themselves against regulatory and reputational risk, according to Ari Redbord, Head of Legal and Government Affairs at TRM Labs—a blockchain intelligence company that works with government, financial institutions, and crypto businesses to track and monitor transactions to mitigate illicit finance risks. According to Redbord, any business considered a Virtual Asset Service Provider (VASP) under the Financial Action Task Force (FATF) definition will almost certainly need to screen for "illicit finance risks such as darknet exposure, terrorist financing, child exploitation, hacks, frauds, and myriad other risks from illicit actors who seek to take advantage of the decentralized, permissionless, fast nature of crypto."

- Nested exchanges like SUEX can be difficult to detect because they often exploit the greater liquidity and lower transaction costs of big, multinational exchanges while presenting customers with a custom-made interface that obscures the connection to the larger service, according to Redbord. TRM clients—including large, regulated exchanges—leverage the company's Ownership Analytics capability to identify parasite exchanges and other nested entities operating on their platforms.

- At the same time, human-driven insight into ownership, control, and other critical factors that inform company engagement decisions and help interpret data is critical. Regional, cultural, and linguistic expertise can help

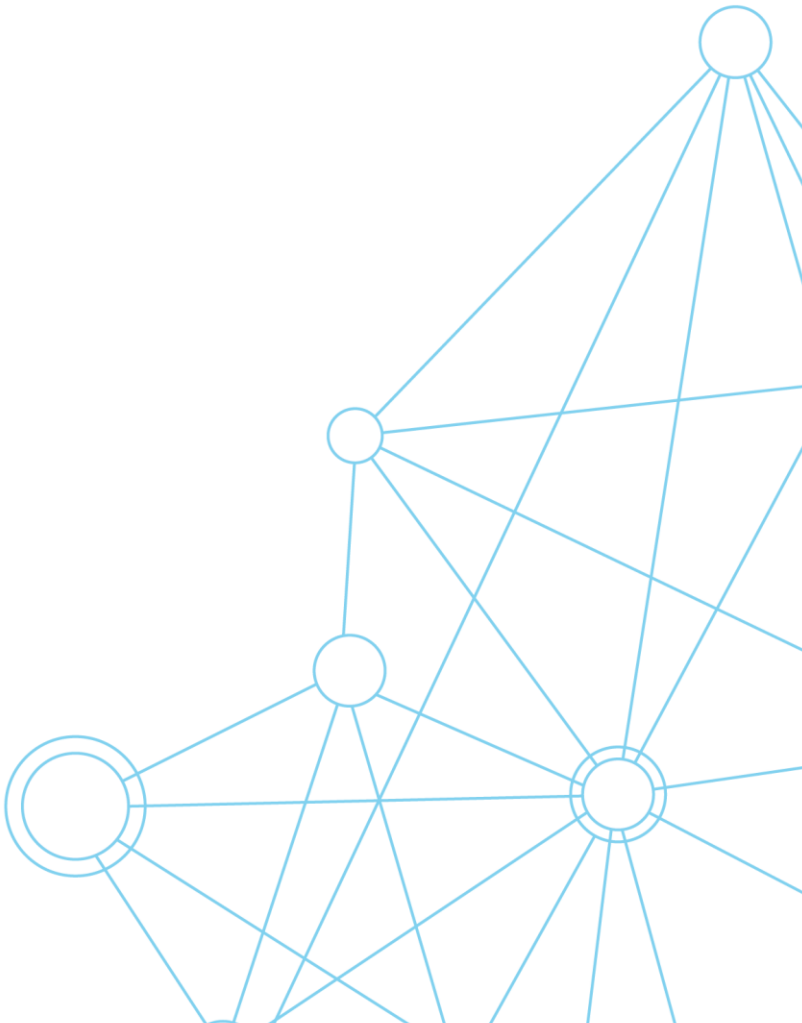
INFO@FIVEBY.COM
206-800-1700
FIVEBY.COM

expose connections between major shareholders and any suspicious individuals and entities, including politically exposed persons (PEPs), possible business activities in risky jurisdictions, complex ownership chains, and questionable business practices to inform business decisions, as well as interpret the reams of data that may be available via technology tools.

The US government's action this week also highlights reputational risks for entities owned or controlled by owners and investors in SUEX. Our research reveals that Belorussian individual Egor Petukhovsky, and three Russians—Maksim Subbotin, Ildar Zakirov, and Vasiliy Zhabykin—are shareholders in the firm, with Zhabykin and Czech venture capitalist Tibor Bokor as members of the board of directors. Insights into these individuals would almost certainly make firms considering doing business with them or entities connected with them more hesitant to engage.

FiveBy is a specialized risk intelligence services firm. We give you the insight you need to move faster and further with the confidence to transform your risks into opportunity. The opportunity to grow your profits, strengthen your brand, and exceed your customer expectations.

Our unique point of view brings together expertise spanning security, technology, data science, and business operations to connect your dots. By turning data into an enabler, FiveBy designs adaptable responses—whether to an ongoing incident or to implement preventive measures—tailored to your business needs and always with a human touch.



INFO@FIVEBY.COM
206-800-1700
FIVEBY.COM