Proskauer

Don’t Get Caught Up in the Mix: OFAC Sanctions Another Crypto Mixer for Potential Violations of Sanctions Regulations and FinCEN Proposes New Rule

Blockchain and the Law on **December 21, 2023**

U.S. government agencies continue to take action against cryptocurrency mixing services that enable cybercriminals to obfuscate the trail of stolen proceeds on public blockchains stemming from illicit cyber activity. On November 29, 2023, the U.S. Department of the Treasury’s Office of Foreign Assets Control (“OFAC”) sanctioned another virtual currency mixing service, Sinbad.io, for “serving as a key money-laundering tool of the OFAC-designated Lazarus Group, a state-sponsored cyber hacking of the Democratic People’s Republic of Korea (“DPRK”).” Sinbad.io, reportedly the second-largest mixer by volume in 2023, allegedly also processed millions of dollars’ worth of virtual currency from the Horizon Bridge and Axie Infinity hacks. Around the same time, European authorities seized the servers of Sinbad.io in the Netherlands and Finland. This is the latest mixer sanctioned by OFAC, with the first being the Blender.io virtual currency mixer back in May 2022, which the agency, at the time, deemed a key money-laundering tool of the Lazarus Group (in fact, OFAC claims that Sinbad.io was a successor to Blender.io). Treasury has shown again that it will aggressively use its powers to disrupt crypto-related financial nodes tied to illicit payments and cyberattacks.

As discussed in numerous articles, most blockchains, including the largest like Bitcoin and Ethereum, are public and transparent, meaning transactions and activity on a public blockchain can be tracked and traced. Crypto mixing services, or mixers, blend users' virtual assets together to obfuscate the origins, destinations and counterparties of the funds and underlying transactions. When used for lawful purposes, proponents note that mixers enable much-needed financial privacy for individuals living under oppressive regimes or simply wish to transact legally — and anonymously. At the same time, governments and law enforcement agencies point out that that mixers are widely used by bad actors to support malicious cyber activities and money-laundering of stolen virtual currency.[1]

Mixers or "tumblers" generally work by blending the assets of many users in a "black box" that hides the assets and then distributing those assets to new addresses. For example, to anonymous transfer assets, Person A transfers assets to the mixer, which then mixes the assets and distributes them to Person B. As with most blockchain technology, there are centralized and decentralized sides of the coin. And as with many technologies that anonymize transactions or communications, they are not necessarily foolproof and law enforcement agencies (or their independent contractors) have the resources to trace certain assets despite the use of masking efforts.

When using a centralized mixer, users trust third-party services to receive the assets, mix such assets with other users' assets, and redistribute them. Decentralized mixers (i.e., open-source protocols) enable an automatic permissionless mixing process. Users send assets to the protocol, which returns a cryptographic key to the sender that allows the sender to designate a destination. In the meantime, the mixer blends transactions. When the sender decides to withdraw the funds from the mixer, the sender returns the cryptographic key, which deposits the assets into a new address.

Mixers are inherently anonymous and obfuscating, which is one reason why OFAC alleged that cybercriminals leveraged Sinbad.io to conceal transactions linked to sanctions evasions, drug trafficking, and other illicit sales on darknet marketplaces. OFAC's action against Sinbad.io comes about a year after sanctions against Tornado Cash for similar offenses (note: In October 2023 a Florida district court held that OFAC's designation of all of the addresses affiliated with Tornado Cash, including the core software tool, did not exceed its statutory powers and was consistent with Treasury regulations; that case is on appeal. A Texas district court earlier in the year rejected a similar challenge; that case is also on appeal). As a result of such sanctions, all property and interests in the property of Sinbad.io and Tornado Cash that are in the United States or the possession and control of U.S. persons must be blocked and reported to OFAC. Engaging in transactions with such designated entities may result in sanctions against such transactors.

OFAC also designated Sinbad.io 41 days after the United States Treasury Department's Financial Crimes Enforcement Network (FinCEN) proposed a rule, which would, if adopted, require covered financial institutions, as defined in 31 C.F.R. 1010.100(t), to implement monitoring and reporting regimes concerning transactions involving mixers. Covered financial institutions have until January 22, 2024, to comment.

OFAC, FinCEN, and other U.S. authorities are increasingly concerned about and focused on crypto mixing activities. In a speech on November 29, 2023, Treasury Deputy Secretary Wally Adeyemo noted the need for the digital asset industry to innovate within the bounds of the law while working to prevent "bad actors from using the digital asset ecosystem for illicit activity." With heightened focus, financial institutions, investors, businesses, and operators must understand the regulatory and legislative regimes applicable to their business and investments.

View Original

---

[1] According to Chainanalysis, in 2022, about 8% of crypto mixer users were linked to illicit accounts, while 0.24% of all cryptocurrency transactions were tied to illicit activity. 2023 Crypto Crime: Illicit Crypto Volumes Reach All-Time Highs – Chainalysis.

Related Professionals

- **Seetha Ramachandran**

Partner