Tornado Cash Sanctions May Signal Enforcement Shift

By **Kara Bombach, Kyle Freeny and David Miller** (September 2, 2022)

Kara Bombach

Kyle Freeny

David Miller

In a move that has shaken the virtual currency industry, the U.S. Department of the Treasury's Office of Foreign Assets Control on Aug. 8 imposed economic sanctions on Tornado Cash, a popular cryptocurrency mixing service that allows customers to obscure the original source of virtual currency transactions by mixing multiple transactions and then redistributing them.

While mixing may have legitimate benefits in some transactions, it also can be exploited by bad actors to potentially launder cryptocurrency, including crypto received in connection with ransomware attacks. This is the first time OFAC has targeted a decentralized software protocol.

OFAC levied the sanctions designation pursuant to Executive Order No. 13694 on malicious cyber activities, which was issued in 2015 the wake of an increase in ransomware attacks and which targets cyber-enabled threats to U.S. national security.

According to OFAC, Tornado Cash was responsible for "launder[ing] the proceeds of cybercrimes," including the equivalent of more than $455 million stolen by the Lazarus Group, a North Korea state-sponsored hacking group that the U.S. sanctioned in 2019.[1]

Among other things, the designation of Tornado Cash has the effect of prohibiting U.S. persons from utilizing the service, as it — and several Ethereum addresses associated with it — has been added to OFAC's list of specially designated nationals.

U.S. Authorities' Increased Attention to Mixers' Role in Money Laundering

In one sense, the move is but the latest signal of U.S. authorities' increased attention on the role that mixers play in the anti-money laundering landscape.

In October 2020, the U.S. Department of Justice struck a cautious note on mixers in its Cryptocurrency Enforcement Framework, warning that operators of mixing services could potentially be criminally liable for money laundering.

Earlier that year, the DOJ charged the operator of Darknet-based mixer Helix, a U.S. citizen, who ultimately admitted the service was targeted to narcotics sales and other illicit transactions.[2]

OFAC's first-ever designation of a mixing service, Blender.io, came in May, roughly three months before Tornado Cash was sanctioned. Like Tornado Cash, Blender.io was alleged to have laundered virtual currency for the Lazarus Group.

The Tornado Cash designation nonetheless marks a potential new front in U.S. authorities' effort to crack down on mixers believed to play a role in laundering money.

Unlike Blender.io and Helix, which offered more traditional centralized mixing services, Tornado Cash is a smart contract-based mixing protocol built on the Ethereum blockchain, and it provides no custodial services.

In March, one of its founders claimed that Tornado Cash's code allows the service to be run indefinitely without any control or maintenance by its developers.

Among the Ethereum addresses sanctioned by OFAC were reportedly addresses for the smart contract responsible for executing the mixing.

Potential Implications for Virtual Currency Enforcement Landscape

The decision to target a decentralized protocol has provoked a response from the decentralized finance industry, which has raised concerns that such targeting will stifle innovation.

Cryptocurrency advocacy group Coin Center has signaled that it is considering a possible legal challenge to the designation. But the Treasury Department has shown no indication that it plans to retreat from its position.

The Tornado Cash example also highlights the uncertainty about mixer developers' potential liability for the actions of their customers, particularly in the case of decentralized protocols capable of operating autonomously.

A few days after OFAC's designation of Tornado Cash, Dutch authorities arrested an alleged developer of the Tornado Cash protocol. But prosecuting a person under U.S. law for money laundering or criminal sanctions violations — for example, related to funds allegedly mixed for North Korean actors — requires proof of criminal intent, whereas civil penalties for sanctions violations can be imposed under a strict liability standard.

Federal authorities may have avoided these thorny issues for now by pursuing an enforcement-through-sanctions approach rather than more traditional criminal or civil penalties.

Indeed, the specially designated national classification may be intended to avoid the potential obstacles to traditional enforcement actions against Tornado Cash and those affiliated with it, including questions about jurisdiction.

OFAC may sanction targets anywhere in the world, whereas prosecutors face jurisdictional constraints, even for laws such as those related to money laundering, which have extraterritorial applications.

The U.S. government typically also has wider discretion and a lower burden to impose economic sanctions against non-U.S. persons.

It remains to be seen whether the move marks a shift in tactics — perhaps a subtle prioritization of disruption over prosecution — or if instead it simply signals that U.S. authorities intend to use the full range of tools at their disposal to target services they believe facilitate money laundering.

Services believed to be leveraged by designated state sponsors of terror, such as North Korea, may be at particular risk.

Compliance Considerations Moving Forward

In a press release announcing its sanctioning of Tornado Cash, OFAC noted that "Treasury will continue to investigate the use of mixers for illicit purposes and use its authorities to respond to illicit financial risks in the virtual currency ecosystem."[3]

OFAC has encouraged all companies in the virtual currency industry — including exchanges, miners, wallet providers, administrators, technology companies and even more traditional financial institutions with virtual currency touchpoints — to employ risk-based sanctions compliance programs.

Virtual currency businesses may wish to review and update, as appropriate, their sanctions compliance programs, as well as their anti-money laundering and countering the financing of terrorism compliance programs.

Cryptocurrency firms should be mindful that sanctioned mixers such as Tornado Cash may still be capable of operating, notwithstanding the fact that they are subject to sanctions. Accordingly, cryptocurrency firms subject to U.S. jurisdiction must take care to ensure that their platforms do not transact with sanctioned entities such as Tornado Cash or accept funds mixed through the service after the date of the designation.

OFAC sanctions violations are subject to a strict liability standard, meaning that no intent, knowledge or reason to know that one is dealing with a sanctioned person is required for a violation to occur.

OFAC has previously noted that firms may consider deploying blockchain analytics tools to help identify and mitigate sanctions risks.

Sanctions compliance is likely to be made more complicated by the decentralized nature of the target. Several web applications have reportedly blocked access to Tornado Cash's front-end application. But an anonymous user still reportedly managed to send small amounts of Ethereum through a sanctioned Tornado Cash wallet to unsuspecting recipients, including several high-profile celebrities and business leaders. These transactions led to temporary suspension of the unsuspecting recipients' accounts as a result of sanctions screening protocols.

It remains to be seen if the sanctions have the desired effect of disrupting criminal actors' use of the protocol. Time will also tell whether Congress will step into the controversy to address the regulation of decentralized applications.

Kara M. Bombach is a shareholder and chair of the Washington, D.C., international trade group at Greenberg Traurig LLP.

Kyle R. Freeny is a shareholder at the firm. She formerly served as a prosecutor with the U.S. Department of Justice's Money Laundering and Asset Recovery Section.

David I. Miller is a shareholder at Greenberg Traurig. He formerly served as assistant U.S. attorney for the Southern District of New York, and as a terrorism prosecutor with the U.S. Department of Justice.

Greenberg Traurig shareholder Marina Olman-Pal, and U.S. data, privacy and cybersecurity practice co-chair Jena M. Valdetero, contributed to this article.

[1] https://home.treasury.gov/news/press-releases/jy0916.

[2] https://www.justice.gov/opa/pr/ohio-resident-pleads-guilty-operating-darknet-based-bitcoin-mixer-laundered-over-300-million.

[3] https://home.treasury.gov/news/press-releases/jy0916.