BANKING
DIGITAL

Digital assets and sanctions compliance: Tornado Cash and beyond

Paul Marquardt, Gabriel Rosenberg and **Will Schisa** of **Davis Polk** explore sanctions compliance challenges and best practices in the digital assets space

On August 8 2022, the US Treasury Department's Office of Foreign Assets Control (OFAC) imposed sanctions on Tornado Cash, a decentralised cryptocurrency "mixer" application that OFAC alleges had been used to launder billions of dollars in proceeds of criminal activity, including proceeds stolen by state-sponsored North Korean hacking groups. The designation of Tornado Cash has proven controversial, with critics of the action accusing OFAC of overreach and censorship and Tornado Cash users filing two lawsuits against OFAC in US federal district court, claiming that the agency's action was not authorised by statute and violates the US Constitution. Notwithstanding this reaction, the Tornado Cash designation was in fact broadly consistent with OFAC's emerging approach to addressing the illicit financing and sanctions evasion risks posed by virtual currency and other digital assets, and the obligations it imposes on those required to comply with US sanctions are not different in kind from those imposed by other sanctions actions OFAC has taken, even if those obligations have been more broadly felt by those acting in or interacting with the digital assets ecosystem than has been the case with respect to previous sanctions actions that have resulted in the public identification of blacklisted virtual currency addresses.

This article addresses sanctions compliance challenges and best practices in the digital assets space, using the Tornado Cash designation as a case study. It will also address the controversy (and related legal challenges) over whether OFAC's action was a lawful and appropriate use of its sanctions authorities.

Economic sanctions and digital assets

The US government uses economic sanctions as a tool to address a variety of threats to the national security, foreign policy, or economy of the US. Sanctions, which are primarily implemented and enforced by OFAC and are authorised under

a number of different enabling statutes, prohibit or regulate transactions subject to US jurisdiction involving proscribed countries or territories, governments, persons, or property. While sanctions may take a number of different forms, the most common type – and the type that was applied with respect to Tornado Cash – is a targeted asset freeze, in which OFAC publicly identifies a particular sanctioned person (or its property) and publishes its name and associated identifiers on the List of Specially Designated Nationals and Blocked Persons (SDN List). All property and property interests of the sanctioned person within US jurisdiction must be frozen, and transactions involving the sanctioned person or its property or property interests are generally prohibited unless licensed by OFAC.

Typically, the obligation to comply with US sanctions extends to "US persons" (individual US citizens or lawful permanent residents, wherever located, entities organised under the laws of the US or any jurisdiction thereof, and persons physically present in the U S), as well as to transactions taking place in whole or in part in the US. OFAC interprets this latter category broadly, and has found non-US persons liable for violating US sanctions by, for example, routing transactions involving sanctioned persons through the US financial system or using US-based servers for such transactions. Sanctions violations are subject to civil and criminal penalties, with OFAC and the US Department of Justice exercising overlapping enforcement jurisdiction and a range of other federal and state regulatory and law enforcement agencies pursuing sanctions violations under other authorities (such as bank regulation, fraud, or anti-money laundering statutes and regulations).

While sanctions compliance obligations apply to digital assets transactions in the same way that they do to any other type of activity, traditional sanctions compliance practices, which are heavily reliant on collection and screening of customer, counterparty, and transaction information by intermediaries, are challenging to adapt to the digital asset context. Disintermediation and the ability to transact anonymously or pseudonymously are common and attractive features of many digital asset business models, but they also create opportunities for sanctions targets, as well as other illicit actors, to transact without being detected and interdicted.

OFAC has published public guidance advising digital asset industry participants on best practices to address these sanctions compliance risks. These include:

- "Know-your-customer" procedures to collect and update identifying information about customers at onboarding and on an ongoing basis in order to conduct due diligence sufficient to mitigate potential sanctions-related risk;
- Conducting sanctions screening against (at minimum) digital wallet addresses associated with sanctioned persons published by OFAC and included on the SDN List, as well as other available identifying information concerning parties to transactions;
- Utilising blockchain analytics linking public information on the blockchain with other sources of information to identify and prevent transactions with other digital wallet addresses that may be associated with sanctioned persons;
- Leveraging IP address or other geolocation information to block persons appearing to be located in sanctioned countries or territories from accessing products or services; and
- Making sanctions risk assessments and the incorporation of appropriate sanctions controls part of the development process for new technologies or **business models**.

While OFAC does not require companies to adopt these or any other specific sanctions compliance practices, the existence and adequacy of a company's risk-based sanctions compliance program is a key factor in OFAC's evaluation of the appropriate enforcement response to an apparent sanctions violation. Apparent sanctions violations by actors that have implemented reasonable compliance programs that are consistent with OFAC's recommended best practices are more likely to be resolved through non-public action, such as the issuance of a cautionary letter. This is consistent with OFAC's broader enforcement practice with respect to financial and non-financial institution targets.

OFAC has reinforced the importance of the best practices described in its guidance through a number of enforcement actions involving actors in the digital assets space. In the past several years, OFAC has announced several settlements with such actors, typically in cases where the target of the enforcement action had access to information that would have allowed it to identify the involvement of a sanctions target in a transaction, but did not act on that information to prevent the transaction. For example, in October 2022, OFAC announced an approximately $25 million settlement with the cryptocurrency exchange **Bittrex**, which OFAC found had operated for an extended period of time without screening customer address and IP location information and thus processed numerous transactions involving persons resident in sanctioned countries or territories. Bittrex also entered into a consent order with the Financial Crimes Enforcement Network (FinCEN) relating to a failure to maintain and adequate anti-money laundering compliance program and file suspicious activity reports during the same **time period**. FinCEN assessed a penalty of approximately $29 million dollars, although the settlement paid to OFAC was applied as an offset. Notwithstanding the number of violations and the extended time period over which they occurred, OFAC found Bittrex's conduct to be non-egregious, and extended substantial mitigation, in large part due to Bittrex's cooperation with OFAC and its extensive efforts to remediate and bring its AML and sanctions compliance programs in line with best practices after the company received inquiries from OFAC and FinCEN in 2017. OFAC's earlier settlements in 2021 with digital currency payments processor BitPay and in 2020 with digital wallet management service provider BitGo involved similar failures to use available IP address and other customer information in fact held by the companies to detect and prevent transactions involving residents of sanctioned countries and territories, albeit on a **smaller scale**.

While adoption of the best practices recommended by OFAC and reinforced though its public enforcement actions may help to mitigate the risk of a sanctions violation and limit potential penalties in the event of such violations, the fact that many digital asset transactions occur with incomplete visibility into the identities of transaction parties creates a vulnerability that cannot be fully addressed by other controls, and that does not exist to the same degree in transactions intermediated by traditional financial institutions. This vulnerability is especially pronounced in the context of so-called decentralised finance (DeFi) applications, which process transactions on an automated basis, are often permissionless, and may not incorporate any sanctions compliance controls.

Tornado Cash as case study

The designation of Tornado Cash is the most recent in a series of sanctions actions by OFAC targeting parts of the digital assets ecosystem that the US government perceives as complicit in facilitating illicit activity involving digital

assets by sanctioned persons, including the receipt of ransomware payments and state-sponsored theft of digital assets. Prior targets have included several cryptocurrency exchanges associated with Russian ransomware activity, as well as the centralized mixing service Blender.io. So-called "mixers" – services or software that accept and commingle cryptocurrency from multiple users and by doing so obfuscate information about the original source of the funds – are a longstanding concern of OFAC and other US government regulators and law enforcement agencies as a result of their obvious utility in laundering the proceeds of illicit activities.

While broadly similar to these prior actions, the designation of Tornado Cash was novel in that it is the first time that OFAC has imposed sanctions against a decentralised protocol. There is no company called "Tornado Cash" that provides virtual currency mixing services to customers; rather, Tornado Cash is a smart contract (i.e., a piece of software code) on the Ethereum blockchain. Much of the commentary around the designation has focused on this aspect, which is certainly important as a policy consideration and relevant to the legal challenge to the action. In particular, many critics of OFAC's action have argued that the agency overreached by targeting autonomous, self-executing code, the behavior of which cannot be changed or deterred by sanctions. While the code itself may be immutable, OFAC's intent appears to be to make the application less effective as a tool for money laundering by barring potential Tornado Cash users who are US persons or otherwise acting within US jurisdiction from interacting with it.

Indeed, from a sanctions compliance standpoint, the distinction between sanctioning a centralised actor and sanctioning a decentralised application is largely irrelevant. The consequences of the Tornado Cash designation are clear – US persons and those acting within US jurisdiction are prohibited from using or interacting with Tornado Cash, including via the virtual wallet and protocol addresses listed on the SDN List, and they must block virtual currency received from or destined for the Tornado Cash application that is or comes within their possession or control. The best practices described above -- particularly screening against proscribed digital asset addresses – straightforwardly address compliance with the Tornado Cash sanctions.

Because Tornado Cash was widely used by US persons, including for purportedly legitimate transactions, and because OFAC identified protocol-level addresses, and not just individual wallets, the designation of Tornado Cash appears to have had a more substantial practical impact than prior OFAC actions targeting virtual currency exchanges and mixers, particularly with respect to freezing of funds of users of the application. OFAC has been criticised for not distinguishing between illicit and legitimate uses of Tornado Cash in applying the sanctions, though the absence of such distinctions is a common feature of asset blocking sanctions, which are a relatively blunt policy instrument. Somewhat belatedly, OFAC has responded to these criticisms by announcing that it would adopt a favourable licensing policy for those seeking complete a transaction or withdraw virtual currency involving Tornado Cash that was deposited prior to its designation, provided that the transaction did not otherwise involve sanctionable conduct. This is a typical step taken by OFAC in to mitigate the harms to innocent parties from significant sanctions actions; the fact that it was not publicised immediately after the Tornado Cash sanctions were announced suggests that OFAC may have not fully understood or anticipated the likely consequences of its actions.

The Tornado Cash designation has proved controversial, with two lawsuits filed to date challenging OFAC's action. The first was brought by a group of six individual Tornado Cash users in the US District Court for the Western District of Texas challenging the designation on statutory and constitutional grounds. The plaintiffs argue that: (1) OFAC did not have the authority to impose the sanctions under the relevant statute, the International Emergency Economic Powers Act (IEEPA), because the Tornado Cash application is not a "person" or "property" OFAC is authorised to regulate under IEEPA; (2) the designation violates the First Amendment by prohibiting users from engaging in protected speech through making anonymous donations to causes they support; and (3) the designation violated the due process cause of the 5th amendment by depriving certain of the plaintiffs of access to their property without sufficient notice and pre-deprivation process. The second lawsuit, filed in US District Court for the Northern District of Florida by the virtual currency research and advocacy organisation Coin Center and three individuals, raises similar claims under the First Amendment and regarding OFAC's statutory authority to designate Tornado Cash and also argues that the designation was arbitrary and capricious because OFAC allegedly failed to fully consider the consequences of its action and acted in a manner inconsistent with established policy without adequate **explanation**.

While litigation is inherently unpredictable and the parties have yet to brief these claims, the constitutional objections raised are ones over which the US government has routinely prevailed in other cases challenging sanctions designations and similar actions. The statutory and administrative procedure arguments raised are more novel, though courts have also traditionally granted OFAC wide latitude to interpret and apply the sanctions authorities it administers. While the cases are certainly worth monitoring, at this time there is no reason to expect that they will result in the overturning of the designation, which remains fully in effect while the litigation is pending.

On November 8, 2022, OFAC **re-designated** *Tornado Cash under both executive order 13694 (the cyber sanctions authority relied upon for the first designation) and executive order 13722, a separate order that authorises the imposition of sanctions on those providing material assistance or support to the North Korean government. OFAC also updated the list of digital asset addresses associated with Tornado Cash on the SDN List. While this does not materially change the scope of the sanctions imposed on Tornado Cash or the related compliance obligations of US persons or those within US jurisdiction, because the action was taken in part under North Korea-related sanctions authorities, these obligations now also extend to non-US entities owned or controlled by US financial institutions – for example, a non-US subsidiary of a US bank.*

OFAC appears to have taken this action in response to the legal challenges to the original designation, as reflected in new ***guidance*** *– presumably now reflected in the administrative record supporting the designation – that clarifies that OFAC considers Tornado Cash to be an entity consisting of the application's founders and developers, as well as the Tornado Cash Decentralised Autonomous Organisation (DAO), and thus a "person" that OFAC has the authority to sanction under IEEPA. The individual founders, developers, and members of Tornado Cash DAO, however, are not themselves sanctioned. By taking this step, OFAC has addressed one of the key statutory arguments raised by the parties challenging the designation, and likely placed itself on a stronger footing to defend against those challenges.*