

UNITED STATES DISTRICT COURT  
WESTERN DISTRICT OF TEXAS  
WACO DIVISION

JOSEPH VAN LOON; TYLER ALMEIDA;  
ALEXANDER FISHER; PRESTON VAN LOON;  
KEVIN VITALE; and NATE WELCH,

Plaintiffs,

- against -

DEPARTMENT OF THE TREASURY; OFFICE OF  
FOREIGN ASSETS CONTROL; JANET YELLEN,  
in her official capacity as Secretary of the Treasury; and  
ANDREA M. GACKI, in her official capacity as Director  
of the Office of Foreign Assets Control,

Defendants.

**AMENDED COMPLAINT**  
No. 6:22-cv-920-ADA-JCM

Plaintiffs Joseph Van Loon, Tyler Almeida, Alexander Fisher, Preston Van Loon, Kevin Vitale, and Nate Welch, for their Amended Complaint against Defendants Department of the Treasury; Office of Foreign Assets Control; Janet Yellen, in her official capacity as Secretary of the Treasury; and Andrea M. Gacki, in her official capacity as Director of the Office of Foreign Assets Control, allege as follows:

**INTRODUCTION**

1. Plaintiffs are users of the Ethereum blockchain. They are also users of a privacy protocol known as Tornado Cash, which consists of open-source software code primarily on the Ethereum blockchain. Plaintiffs bring this action to challenge Defendants' addition of Tornado Cash to the Specially Designated Nationals and Blocked Persons (SDN) List. That unprecedented, overbroad action exceeds Defendants' statutory authority, infringes on Plaintiffs' constitutional

rights, and threatens the ability of law-abiding Americans to engage freely and privately in financial transactions.

2. Ethereum is a public blockchain in which nodes cooperate through a peer-to-peer network to maintain and build a transparent, distributed ledger. The blockchain essentially operates as a cooperative, transparent network. Users of Ethereum install an application called a wallet, which generates addresses for the user and a private key that functions like a password. Users can send and receive Ether (ETH) and other crypto assets without the involvement of any intermediary.

3. Transactions are grouped into blocks. As each block is added to the chain, it points to the block before it, forming a chain of blocks. The blocks are publicly and permanently recorded on the Ethereum blockchain. Ethereum's transparency allows verification of transactions, but it also makes it difficult for users to protect their privacy if a third party connects an Ethereum address with their real-world identity.

4. Tornado Cash is not a person, entity, or organization. It is a decentralized, open-source software project that restores some privacy for Ethereum users. Software code is a string of letters and numbers that perform a specific function. Open-source code can be used or distributed by anyone. The code at issue in this case was developed over many years by a large group of individual contributors, which was made available as open-source code and published as a collection of smart contracts on the Ethereum blockchain.

5. A smart contract is a program stored on the blockchain that runs when predetermined conditions are met. Once a smart contract is deployed on the Ethereum blockchain, it is assigned a public address with which any user can interact. When an individual user interacts with a smart contract, the code automatically carries out a particular, predetermined task without any human intervention.

6. The most important Tornado Cash smart contracts are called pools. A user can deposit Ether or other crypto assets from one crypto address into the pool and then withdraw that same asset to a different address, including one that has never been used or associated with the user. Users can withdraw only the assets they deposited, using a secret “key” that the smart contract creates and verifies. Although transactions with the pool are publicly recorded, the pool provides a degree of privacy by permitting individuals to withdraw assets into another address of their choice, making it less likely to be attributed to the user. The Tornado Cash pools presently in use are immutable.

7. On August 8, 2022, Defendants added Tornado Cash to the SDN List, listing the website [tornado.cash](https://tornado.cash), 37 Tornado Cash smart contracts, and an address that was used to accept donations to develop Tornado Cash projects.<sup>1</sup>

8. On September 8, 2022, Plaintiffs filed a complaint in this Court challenging Defendants’ designation.

9. On November 8, 2022, on the eve of the deadline to respond to the complaint, Defendants revoked their August 8, 2022, action adding Tornado Cash to the SDN List and simultaneously re-added Tornado Cash to the SDN List. Once again, Defendants’ designation of Tornado Cash listed the website [tornado.cash](https://tornado.cash), the donation address, and all of the original Tornado Cash smart contracts except one obsolete smart contract. Defendants also added 53 smart contracts. The November 8, 2022, redesignation wholly replaced the August 8, 2022, designation and invoked additional legal authority. Defendants did not cite any intervening event for their decision.

10. The President has delegated certain sanctions authority to Defendants, but that authority is limited and does not extend to the listing of Tornado Cash and the Tornado Cash smart

---

<sup>1</sup> The initial designation listed 45 Ethereum addresses, but several of them were duplicates.

contracts. For example, the President may sanction activities involving “any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States.” 50 U.S.C. § 1702(a)(1)(B). The President may also sanction “any person” who knowingly engages in certain conduct relating to North Korea. *See* 22 U.S.C. § 9214. Moreover, “whenever the United States is called upon by the [United Nations] Security Council,” the President may sanction “economic relations or rail, sea, air, postal, telegraphic, radio, and other means of communication between any foreign country or any national thereof or any person therein and the United States or any person subject to the jurisdiction thereof, or involving any property subject to the jurisdiction of the United States.” 22 U.S.C. § 287c(a).

11. Tornado Cash is not property, a foreign country or a national thereof, or a person of any kind. And the Tornado Cash smart contracts, which consist of open-source software code, are not any of the foregoing or an identifier of any of the foregoing.

12. Plaintiffs seek declaratory and injunctive relief under the United States Constitution and the Administrative Procedure Act (APA), 5 U.S.C. §§ 500 *et seq.*, to remedy Defendants’ unlawful action. OFAC’s designation exceeds its statutory authority and is not in accordance with law. *See* 5 U.S.C. § 706(2)(A), (C). OFAC’s designation is also unconstitutional under the Free Speech Clause of the First Amendment to the U.S. Constitution and the Due Process Clause of the Fifth Amendment to the U.S. Constitution. *See* 5 U.S.C. § 706(2)(B). Plaintiffs respectfully request that this Court hold the designation unlawful, set it aside, and permanently enjoin its enforcement.

### **JURISDICTION AND VENUE**

13. This action arises under the U.S. Constitution and the APA, 5 U.S.C. §§ 500 *et seq.* This Court has jurisdiction pursuant to 28 U.S.C. § 1331.

14. Venue is proper in this District pursuant to 28 U.S.C. § 1391(e)(1) because Plaintiff Joseph Van Loon resides in Cedar Park, Texas, within the Western District of Texas, and Defendants are agencies or officers or employees of the United States acting in their official capacities.

### **PARTIES**

15. Plaintiff Joseph Van Loon is an American citizen and a resident of Cedar Park, Texas. He is an application security engineer at an international technology company, where he performs threat modeling and security testing for applications. He previously worked as an application security engineer at Amazon.

16. Mr. Van Loon owns crypto assets. He has a public Ethereum Name Service (ENS) name that can be traced to him. ENS names are often a person's real name, such as JohnDoe.eth, or are otherwise publicly tied to that person's identity. They are linked to that individual's wallet address.

17. In October 2021, Mr. Van Loon used Tornado Cash to send money to a new, more private wallet address. He did so in anticipation of running an Ethereum validator node, which involves depositing Ether to activate software to validate Ethereum transactions. By adding new blocks to the blockchain, validators earn Ether. The process of running validator nodes is called staking. Running a new validator node is thus a valuable activity, but it may also attract attention from malicious actors. Mr. Van Loon ultimately decided to delay his plan.

18. In early August 2022, Mr. Van Loon resumed his plan to run a new validator node. He intended to use Tornado Cash to anonymize his transfer of crypto assets and avoid the attention of malicious actors. After OFAC's August 8, 2022, designation, he abandoned his plan to run the validator node and lost out on the potentially valuable opportunity to earn Ether.

19. Mr. Van Loon has used Tornado Cash because he believes its privacy protocols are safe and because it is integrated into the Ethereum blockchain. He is not confident that alternative

protocols would be as safe and convenient. He would use Tornado Cash again to run a validator node or make investments if Tornado Cash were no longer designated.

20. Plaintiff Tyler Almeida is an American citizen and a resident of the state of California. Mr. Almeida is a senior security risk analyst at Coinbase, the largest cryptocurrency exchange platform in the United States. In that capacity, Mr. Almeida works with threat modelers and vulnerability assessors to identify and quantify security and privacy risks for the company, and design compensating controls to mitigate those risks. He is a Certified Information Systems Security Professional.

21. Mr. Almeida owns crypto assets. He maintains a public crypto wallet address that can be traced to him. In March 2022, following Russia's invasion of Ukraine, Mr. Almeida decided to donate relief funds to the Ukrainian government's publicly posted crypto wallet address. Mr. Almeida wanted to make his donation anonymous and was afraid that crypto wallets that donated to Ukraine's public address (and addresses associated with those donor wallet addresses) would be targeted by Russian state-sponsored hacking groups. To anonymize his donation and prevent his financial history from being associated with his political views, Mr. Almeida sent 0.5 ETH to Tornado Cash, which is worth approximately \$600 today. Mr. Almeida used 0.2 ETH of the cryptocurrency he sent to Tornado Cash to make a donation that would be worth approximately \$250 today.

22. Since his donation, the anonymized wallet address that he established to make the donation has received unwanted air drops of non-fungible tokens from potentially malicious external sources. Like e-mail spam, those air drops are disruptive and potentially part of a scam.

23. A portion of Mr. Almeida's property—0.3 ETH, worth approximately \$350 today—remains locked in Tornado Cash smart contracts. Those funds are now blocked—effectively

trapped—pursuant to OFAC’s sanctions. Following OFAC’s designation of Tornado Cash, U.S. persons are prohibited from dealing with the smart contracts, even to withdraw their own funds. Mr. Almeida would use Tornado Cash again in the future if it were not designated, both to recover his funds and to make future transactions while protecting his privacy and security. Among other things, he is concerned about the potential for his financial history to be used as part of a spam-and-scam scheme that could enable malicious actors to gain access to his private or work accounts.

24. Plaintiff Alexander Fisher is an American citizen and a resident of the state of Michigan. Mr. Fisher manages blockchain and decentralized application infrastructure, with a focus on the Ethereum network. Mr. Fisher previously worked as a network operations specialist and corporate webcasting leader at Ford Motor Company.

25. Mr. Fisher owns crypto assets and purchased his first Bitcoin using Coinbase on or about January 2, 2014. Mr. Fisher has a large presence in the Ethereum community and posts his public ENS name on his public Twitter profile. Mr. Fisher has concerns about hacking, and he wants to protect the safety of his family. In the past, people have been able to use public data sources to find Mr. Fisher’s wallet addresses. Until recently, he could use Tornado Cash to protect his security and privacy while transacting, including to obtain funds for staking and for personal transactions.

26. Mr. Fisher and Plaintiff Kevin Vitale have written proof-of-concept code that used the open-source Tornado Cash code to allow those who stake Ethereum to have greater security and privacy. In 2021, their innovative smart contract was awarded a first-place prize at ETHDenver, a member-owned community innovation festival.

27. If Tornado Cash were not designated, Mr. Fisher would use it to continue transacting for staking and personal purposes while protecting his privacy and security. He is now unwilling to interact with the software out of fear of serious penalties for violating OFAC sanctions.

28. Plaintiff Preston Van Loon is an American citizen and a resident of the state of Tennessee. He is the co-founder of Prismatic Labs, which describes itself as a “grassroots team of software engineers all around the world building the code behind the Ethereum blockchain.” *See* Prismatic Labs <prismaticlabs.com> (last visited Nov. 21, 2022). The mission of Prismatic Labs is to “build[] a more fair, open, and censorship-resistant Internet.” *Id.* Mr. Van Loon previously worked as a software engineer at Google.

29. Mr. Van Loon owns crypto assets and maintains a public ENS name that could be traced to him. He has used Tornado Cash on five occasions to protect his privacy and security. Using Tornado Cash allows him to execute personal transactions without connecting them to his publicly known wallet address. It also allows him to experiment with decentralized applications to pursue new crypto business models without connecting them to his publicly known wallet address and personal identity.

30. Mr. Van Loon currently has approximately 1.3 ETH trapped in Tornado Cash as a result of OFAC’s designations, which is worth approximately \$1,500 today. He would use Tornado Cash again if it were not designated, both to access those funds and to continue engaging in personal transactions and experiments with decentralized applications.

31. Plaintiff Kevin Vitale is an American citizen and a resident of the state of Michigan. Mr. Vitale is a principal crypto engineer at GridPlus, where he manages, hires, and expands the company’s engineering team and provides strategic direction to the company. He also owns and operates a small business, where he is a blockchain network engineer who manages infrastructure



for Ethereum-staking and other related blockchain activities. Mr. Vitale has previously worked as a software-development consultant at TD Ameritrade; a senior software engineer at Duo Security, which is now owned by Cisco Systems; and head of mobile development at Domino's.

32. Mr. Vitale owns crypto assets. As part of his job, he has a public ENS name that is posted to his public Twitter profile. Mr. Vitale has concerns about his privacy and safety because malicious actors could target the assets generated by his Ethereum-staking business. Those concerns are not speculative. In 2021, a contractor working in the vicinity of the location where he engages in staking realized that Mr. Vitale staked Ether and asked how much money he made. He worries that other strangers could follow his transaction patterns on the Ethereum blockchain and identify the valuable crypto assets in his possession.

33. When OFAC designated Tornado Cash in August 2022, Mr. Vitale had imminent plans to transfer 10 ETH, or approximately \$11,500, to Tornado Cash for future investments in business opportunities maintaining Ethereum infrastructure. He was prevented from doing so by OFAC's designation.

34. If Tornado Cash were not designated, Mr. Vitale would continue using it for personal purposes and for funding his business operations while protecting his privacy and security.

35. Plaintiff Nate Welch is an American citizen and a resident of the state of Maine. Mr. Welch currently works as a senior software engineer at Coinbase. He maintains the company's crypto wallet, which is used to manage customer withdrawals and deposits.

36. Mr. Welch owns crypto assets. As part of his job, he maintains a public ENS name that is posted to his public Twitter profile. To protect his privacy and security, Mr. Welch has used Tornado Cash on at least six different occasions to avoid harassment from malicious actors. Although Mr. Welch has used other crypto privacy tools, he prefers Tornado Cash because it has

the highest volume of users and transactions, which ensures greater anonymity by making it more difficult to trace particular Ether to particular users.

37. Mr. Welch has 1.2 ETH trapped in Tornado Cash as a result of OFAC's designation, which is worth approximately \$1,400 today. Mr. Welch would use Tornado Cash again if it were not designated by OFAC, both to access his trapped funds and to continue transacting privately and securely.

38. None of the Plaintiffs is a terrorist or a criminal. None launders money. None is a member of the government of North Korea or the North Korean Workers' Party. None supports terrorism, illegal activity, the government of North Korea, or the Korean Workers' Party. Each is an American who simply wants to engage in entirely lawful activity in private.

39. Defendants are the Department of the Treasury; OFAC; Janet Yellen, in her official capacity as Secretary of the Treasury; and Andrea M. Gacki, in her official capacity as Director of OFAC. The Department of the Treasury is a federal administrative agency; OFAC is a federal administrative agency within the Department of the Treasury. Both the Department of the Treasury and OFAC are headquartered in Washington, D.C. Defendants Yellen and Gacki acted under color of law at all relevant times.

### **THE ETHEREUM BLOCKCHAIN**

40. Ethereum is a blockchain platform that supports the cryptocurrency Ether, other crypto assets, and other applications.

41. Ethereum and other blockchains are immutable, public ledgers consisting of a decentralized series of data blocks chronologically linked in a chain. The blockchain is shared over a peer-to-peer network, which makes it public and unable to be altered by any single user. Unlike a traditional ledger, a blockchain ledger reflects every transaction that has ever occurred on that blockchain.

42. The transparency of the blockchain is possible because of cryptography. When individuals transact on the blockchain, they do so using public and private keys generated by an application called a wallet. The public key is an address that users can share with others to send and receive money. The private key is a secret string of letters and numbers that operates as a password to sign transactions that can be verified as valid against an account's public key. Private and public keys are linked, and the blockchain ledger transparently reflects the transaction history of the public keys. *See, e.g., What Is a Private Key?*, Coinbase <[coinbase.com/learn/crypto-basics/what-is-a-private-key](https://coinbase.com/learn/crypto-basics/what-is-a-private-key)> (last visited Nov. 21, 2022).

43. The public nature of that ledger is a crucial feature of the blockchain. It allows two users transacting in crypto assets to ensure that the sender possesses the crypto asset being transacted. Anyone may view the balances and transaction history records of users.

44. The transparency of the blockchain also compromises individual privacy. Because all records are transparent and all transactions are linked, a user's complete financial history—including all prior transactions—can be identified when the accounts involved in a transaction are linked to identities.

45. Although a user can create an anonymized wallet address—one that is not publicly linked to that user—if the user transfers assets from his publicly identifiable address or otherwise links his publicly identifiable address to the anonymous address, a third party can use those transactions or links between a user's wallets to identify that user and his assets. If a user transacts from a publicly identifiable address, or links his anonymous address to one that is publicly associated with the user, third parties have access to a tremendous amount of personal transaction and financial information related to that user.

### **TORNADO CASH**

46. Tornado Cash is an open-source, decentralized, non-custodial privacy protocol primarily on the Ethereum blockchain.

47. Tornado Cash consists of open-source code known as smart contracts that were uploaded by independent developers over the course of years. Smart contracts are software programs stored on the blockchain that self-execute in response to a transaction signed by a private key. Unless their developers include a feature permitting updates, they cannot be altered or controlled once they are uploaded to the blockchain.

48. Since 2020, the backbone of Tornado Cash has been perpetually self-executing code, primarily on the Ethereum blockchain, that cannot be altered, edited, or otherwise controlled.

49. The smart contracts that make up Tornado Cash allow users to deposit tokens from one address and later withdraw the same tokens—and only those same tokens—for deposit in another address. Although both the deposit and withdrawal are visible on Ethereum’s ledger, the ledger does not reflect that the deposit and the withdrawal are linked to the same user. The severing of that link means that an individual can make a withdrawal without exposing his entire financial history to third parties.

50. Tornado Cash is not the only crypto privacy protocol. One feature that sets Tornado Cash apart is its high volume of users and transactions, which protects an individual’s privacy by making it more difficult to match deposits and withdrawals. Another advantage of Tornado Cash is its reputation for security and privacy. A third is the fact that it is non-custodial, so users never surrender or share ownership of their crypto assets.

### **DEFENDANTS’ AUTHORITY TO IMPOSE SANCTIONS**

51. Under the International Emergency Economic Powers Act (IEEPA), the President has authority to take certain actions after “declar[ing] a national emergency with respect to” an

“unusual and extraordinary threat, which has its source in whole or substantial part outside the United States, to the national security, foreign policy, or economy of the United States.” 50 U.S.C. § 1701(a). After making a declaration, the President may take a broad range of actions. 50 U.S.C. § 1702(a)(1). Specifically, the President may, “under such regulations as he may prescribe, by means of instructions, licenses, or otherwise . . . investigate, block during the pendency of an investigation, regulate, direct and compel, nullify, void, prevent or prohibit, any acquisition, holding, withholding, use, transfer, withdrawal, transportation, importation or exportation of, or dealing in, or exercising any right, power, or privilege with respect to, or transactions involving, any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States.” 50 U.S.C. § 1702(a)(1).

52. Under the United Nations Participation Act of 1945, “whenever the United States is called upon by the [United Nations] Security Council,” the President has authority to “investigate, regulate, or prohibit, in whole or in part, economic relations or rail, sea, air, postal, telegraphic, radio, and other means of communication between any foreign country or any national thereof or any person therein and the United States or any person subject to the jurisdiction thereof, or involving any property subject to the jurisdiction of the United States.” 22 U.S.C. § 287c(a).

53. Under the North Korea Sanctions and Policy Enhancement Act of 2016, the President has the authority to designate “any person” engaged in certain enumerated conduct relating to North Korea. 22 U.S.C. § 9214.

54. On April 1, 2015, President Obama issued Executive Order 13,694, which declared a national emergency with respect to “malicious cyber-enabled activities.” 80 Fed. Reg. 18,077 (Apr. 2, 2015). Executive Order 13,694 authorizes the Secretary of the Treasury to identify certain “person[s]” involved in malicious cyber-enabled activities. *Id.* at 18,077-18,078. It also provides

that “property and interests in property” of any of those identified persons would be “blocked,” meaning the property “may not be transferred, paid, exported, withdrawn, or otherwise dealt in.” *Id.* Executive Order 13,694 further delegates to the Secretary of the Treasury “all powers granted to the President by IEEPA as may be necessary to carry out the purposes” of the order. *Id.* at 18,079. The Secretary of Treasury in turn delegated that authority to the Director of OFAC, which maintains the SDN List. *See* 31 C.F.R. § 578.802.

55. On March 15, 2016, President Obama issued Executive Order 13,722. 81 Fed. Reg. 14,943 (Mar. 18, 2016). That order authorizes the Secretary of the Treasury, in consultation with the Secretary of State, to sanction “any person” engaged in certain enumerated conduct relating to North Korea. *Id.* It also provides that “[a]ll property and interests in property” of any of those identified persons should be “blocked,” meaning the property “may not be transferred, paid, exported, withdrawn, or otherwise dealt in.” *Id.* Executive Order 13,722 further delegates to the Secretary of the Treasury “all powers granted to the President by IEEPA and the [United Nations Participation Act] as may be necessary to carry out the purposes of th[e] order.” *Id.* at 14,945. The Secretary of Treasury in turn delegated that authority to the Director of OFAC. *See* 31 C.F.R. § 510.802.

56. Historically, Defendants have used their delegated authority to designate individuals, corporations, other entities, and property on the SDN List. For instance, on February 25, 2022, OFAC added Vladimir Putin to the SDN List. *See Russia-Related Designations*, OFAC (Feb. 25, 2022) <[home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220225\\_33](https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220225_33)>. OFAC also added Kim Jong Un to the SDN List on July 6, 2016. *See Treasury Sanctions North Korean Senior Officials and Entities Associated with Human Rights Abuses*, OFAC (July 6, 2016) <[home.treasury.gov/news/press-releases/jl0506](https://home.treasury.gov/news/press-releases/jl0506)>.

57. Defendants have also designated Blender.io, a virtual currency mixer. *See Cyber-Related Designation; North Korea Designation Update*, OFAC (May 6, 2022) <[home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220506](https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220506)>. Unlike Tornado Cash, Blender.io is operated under centralized control. Also unlike Tornado Cash, users of Blender.io do not retain ownership of particular crypto assets at all times and instead receive randomly “mixed” crypto assets.

58. Although OFAC has procedures by which a designated person can apply for delisting, no such application is possible here because open-source code is not owned by anyone.

### **DEFENDANTS’ DECISION TO DESIGNATE TORNADO CASH**

59. On August 8, 2022, OFAC announced that Defendants had designated Tornado Cash, listing the website [tornado.cash](https://tornado.cash) and 38 Ethereum addresses (some of which were listed more than once), for inclusion on the SDN List. *See U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash*, OFAC (Aug. 8, 2022) <[home.treasury.gov/news/press-releases/jy0916](https://home.treasury.gov/news/press-releases/jy0916)>. The designation was made under Executive Order 13,694, as amended, related to cybersecurity. *See id.* The Defendants noted that North Korea-backed hackers known as the Lazarus Group had used Tornado Cash in April 2022. *See id.*; *see also* 87 Fed. Reg. 49,652 (Aug. 11, 2022).

60. On September 8, 2022, Plaintiffs commenced this action challenging OFAC’s August 8, 2022, designation of Tornado Cash for inclusion on the SDN List.

61. Less than a week later, on September 13, 2022, OFAC published a series of Frequently Asked Questions (FAQs) addressing the designation. *See Frequently Asked Questions* (Sept. 13, 2022) <[home.treasury.gov/policy-issues/financial-sanctions/faqs/added/2022-09-13](https://home.treasury.gov/policy-issues/financial-sanctions/faqs/added/2022-09-13)>. In the FAQs, OFAC described its action as “designat[ing] the entity Tornado Cash.” *Id.* OFAC further stated that, “[a]s part of the SDN List entry for Tornado Cash, OFAC included as identifiers

certain virtual currency wallet addresses associated with Tornado Cash.” *Id.* OFAC stated that “engaging in any transaction with Tornado Cash or its blocked property or interests in property is prohibited for U.S. persons.” *Id.*

62. On November 8, 2022, three months after the original designation and less than a week before the deadline for Defendants to file a responsive pleading, they withdrew their previous designation and “simultaneously redesignated” Tornado Cash. *See Treasury Designates DPRK Weapons Representatives: Tornado Cash Redesignated with Additional DPRK Authorities, New OFAC Guidance* (Nov. 8, 2022) <[home.treasury.gov/news/press-releases/jy1087](https://home.treasury.gov/news/press-releases/jy1087)>. The new designation was made under both Executive Order 13,694 (relating to cybersecurity) and Executive Order 13,722 (relating to North Korea). *See id.* Defendants did not cite any intervening event as the reason for their withdrawal of the original designation and simultaneous issuance of the new designation. As with the August 8, 2022, designation, Defendants’ press release noted that the Lazarus Group had used Tornado Cash in April 2022. *See id.*; *see also* 87 Fed. Reg. 68,578 (Nov. 15, 2022).

63. Also on November 8, 2022, OFAC posted new and revised FAQs on its website. One new FAQ stated that Defendants were “designat[ing] the entity Tornado Cash.” *Frequently Asked Questions* (Nov. 8, 2022) <[home.treasury.gov/policy-issues/financial-sanctions/faqs/1095](https://home.treasury.gov/policy-issues/financial-sanctions/faqs/1095)>. OFAC elaborated that Tornado Cash is a “person” subject to designation under Executive Order 13,694 and Executive Order 13,722, because those orders define “person” to include an “entity,” which is defined as a “partnership, association, trust, joint venture, corporation, group, subgroup, or other organization.” *Id.* OFAC stated that “Tornado Cash’s organizational structure consists of: (1) its founders and other associated developers, who together launched the Tornado Cash mixing service, developed new Tornado Cash mixing service features, created the Tornado



Cash Decentralized Autonomous Organization (DAO), and actively promoted the platform’s popularity in an attempt to increase its user base; and (2) the Tornado Cash DAO, which is responsible for voting on and implementing new features created by the developers.” *Id.* Defendants purported not to designate “Tornado Cash’s individual founders, developers, members of the DAO, or users, or other persons involved in supporting Tornado Cash at this time,” but still purported to block “all Tornado Cash property and interests in property.” *Id.*

64. Notwithstanding OFAC’s designation, Tornado Cash is a decentralized, open-source privacy protocol—not a person, entity, or organization. No person or group of people controls Tornado Cash. No person or group of people—not even the original developers of Tornado Cash—can remove or modify Tornado Cash. Anyone with an internet connection can develop code and add it to the Tornado Cash privacy tool. And anyone with an internet connection can use Tornado Cash.

65. The Tornado Cash smart contracts are not a foreign country or a national thereof, a person of any kind, or the property of any person or country. The Tornado Cash smart contracts are also not identifiers for any person, country, or property.

66. All but one of the listed addresses is a smart contract. Defendants’ action represents the first time that they have added a privacy protocol, smart contract, or open-source code to the SDN List.

67. Twenty-eight of the addresses designated by OFAC are inalterable Tornado Cash smart contracts known as pools that, upon information and belief, were still in use at the time they were added to the SDN List. Of those, eight allow users to deposit and withdraw funds in increments of 0.1, 1, 10, and 100 Ether (ETH) on the Ethereum blockchain and other blockchains;<sup>2</sup>

---

<sup>2</sup> Those addresses are as follows:

eleven allow users to deposit and withdraw funds in increments of other cryptocurrencies on the Ethereum blockchain, namely DAI, USDC, USDT, and WBTC;<sup>3</sup> four allow users to deposit and withdraw funds in increments of other cryptocurrencies on their native blockchains, namely MATIC on the Polygon blockchain, AVAX on the Avalanche blockchain, and xDAI on the Gnosis chain;<sup>4</sup> and five allow users to deposit increments of cDAI tokens, which represent the value of a deposit on a decentralized cryptocurrency borrowing and lending protocol.<sup>5</sup>

---

0x12D66f87A04A9E220743712cE6d9bB1B5616B8Fc  
 0x47CE0C6eD5B0Ce3d3A51fdb1C52DC66a7c3c2936  
 0x910CbD523D972eb0a6f4cAe4618aD62622b39DbF  
 0xA160cdAB225685dA1d56aa342Ad8841c3b53f291  
 0x84443cfd09a48af6ef360c6976c5392ac5023a1f  
 0xd47438c816c9e7f2e2888e060936a499af9582b3  
 0x330bdfade01ee9bf63c209ee33102dd334618e0a  
 0x1e34a77868e19a6647b1f2f47b51ed72dede95dd.

<sup>3</sup> Those addresses are as follows:

0xD4B88Df4D29F5CedD6857912842cff3b20C8Cfa3  
 0xFD8610d20aA15b7B2E3Be39B396a1bC3516c7144  
 0x07687e702b410Fa43f4cB4Af7FA097918ffD2730  
 0x23773E65ed146A459791799d01336DB287f25334  
 0x4736dCf1b7A3d580672CcE6E7c65cd5cc9cFBa9D  
 0xd96f2B1c14Db8458374d9Aca76E26c3D18364307  
 0x0836222F2B2B24A3F36f98668Ed8F0B38D1a872f  
 0x169AD27A470D064DEDE56a2D3ff727986b15D52B  
 0x178169B423a011fff22B9e3F3abeA13414dDD0F1  
 0x610B717796ad172B316836AC95a2ffad065CeaB4  
 0xbB93e510BbCD0B7beb5A853875f9eC60275CF498.

<sup>4</sup> Those addresses are as follows:

0xdf231d99ff8b6c6cbf4e9b9a945cbacef9339178  
 0xaf4c0b70b2ea9fb7487c7cbb37ada259579fe040  
 0xaf8d1839c3c67cf571aa74B5c12398d4901147B3  
 0xa5c2254e4253490c54cef0a4347fddb8f75a4998.

<sup>5</sup> Those addresses are as follows:

0x22aaA7720ddd5388A3c0A3333430953C68f1849b  
 0x03893a7c7463AE47D46bc7f091665f1893656003  
 0x2717c5e28cf931547B621a5dddb772Ab6A35B701  
 0xD21be7248e0197Ee08E0c20D4a96DEBdaC3D20Af  
 0xBA214C1c1928a32Bffe790263E38B4Af9bFCD659.

68. Those twenty-eight inalterable pools form the backbone of Tornado Cash. They consist only of open-source code, and they cannot be modified, deleted, or otherwise controlled by any person or country.

69. Twelve other addresses in OFAC's designation are smart contracts that, upon information and belief, are obsolete, were rarely used, or were never used.<sup>6</sup>

70. The remaining addresses in OFAC's designation concern other features of Tornado Cash:

- a. Two of the addresses designated by OFAC are smart contracts that allow users to transact with TORN, the native token for Tornado Cash.<sup>7</sup> Those smart contracts also allow users to check the total supply of TORN, among other things.
- b. Nineteen of the addresses in OFAC's designation are smart contracts that govern and record the structure and operation of Tornado Cash, including by verifying interactions with the Tornado Cash smart contracts.<sup>8</sup> Upon

---

<sup>6</sup> Those addresses are as follows:

0xF60dD140cFf0706bAE9Cd734Ac3ae76AD9eBC32A  
 0xb1C8094B234DcE6e03f10a5b673c1d8C69739A00  
 0x1356c899D8C9467C7f71C195612F8A395aBf2f0a  
 0xA60C772958a3eD56c1F15dD055bA37AC8e523a0D  
 0xaEaaC358560e11f52454D997AAFF2c5731B6f8a6  
 0xD691F27f38B395864Ea86CfC7253969B409c362d  
 0x9AD122c22B14202B4490eDAf288FDb3C7cb3ff5E  
 0xF67721A2D8F736E75a49FdD7FAd2e31D8676542a  
 0x722122dF12D4e14e13Ac3b6895a86e84145b6967  
 0x94a1b5cdb22c43faab4abeb5c74999895464ddaf  
 0xb541fc07bc7619fd4062a54d96268525cbc6ffef  
 0x527653ea119f3e6a1f5bd18fbf4714081d7b31ce.

<sup>7</sup> Those addresses are as follows:

0x77777feddddfc19ff86db637967013e6c6a116c  
 0x3efa30704d2b8bbac821307230376556cf8cc39e.

<sup>8</sup> Those addresses are as follows:

information and belief, those smart contracts were still in use at the time they were added to the SDN List. At least four of those smart contracts are inalterable.

- c. Nineteen of the addresses in OFAC's designation are smart contracts on a network that developers use to test smart contracts before launching them on the main Ethereum blockchain.<sup>9</sup>

---

0xdf3a408c53e5078af6e8fb2a85088d46ee09a61b  
 0x743494b60097a2230018079c02fe21a7b687eaa5  
 0x653477c392c16b0765603074f157314cc4f40c32  
 0x88fd245fedec4a936e700f9173454d1931b4c307  
 0x09193888b3f38c82dedfda55259a82c0e7de875e  
 0x746aebc06d2ae31b71ac51429a19d54e797878e9  
 0x5f6c97c6ad7bdd0ae7e0dd4ca33a4ed3fdabd4d7  
 0xf4b067dd14e95bab89be928c07cb22e3c94e0daa  
 0xcee71753c9820f063b38fdb4cfdaf1d3d928a80  
 0x5efda50f22d34f262c29268506c5fa42cb56a1ce  
 0x2f50508a8a3d323b91336fa3ea6ae50e55f32185  
 0xffbac21a641dcfe4552920138d90f3638b3c9fba  
 0x179f48c78f57a3a78f0608cc9197b8972921d1d2  
 0x01e2919679362dfbc9ee1644ba9c6da6d6245bb1  
 0xb20c66c4de72433f3ce747b58b86830c459ca911  
 0x2573bac39ebe2901b4389cd468f2872cf7767faf  
 0xca0840578f57fe71599d29375e16783424023357  
 0x58e8dcc13be9780fc42e8723d8ead4cf46943df2  
 0xd90e2f925da726b50c4ed8d0fb90ad053324f31b.

<sup>9</sup> Those addresses are as follows:

0x6bf694a291df3fec1f7e69701e3ab6c592435ae7  
 0x3aac1cc67c2ec5db4ea850957b967ba153ad6279  
 0x723b78e67497e85279cb204544566f4dc5d2aca0  
 0x0e3a09dda6b20afbb34ac7cd4a6881493f3e7bf7  
 0x76d85b4c0fc497eccc38902397ac608000a06607  
 0xcc84179ffd19a1627e79f8648d09e095252bc418  
 0xd5d6f8d9e784d0e26222ad3834500801a68d027d  
 0x407cceeaa7c95d2fe2250bf9f2c105aa7aafb512  
 0x833481186f16cece3f1eeea1a694c42034c3a0db  
 0xd8d7de3349ccaa0fde6298fe6d7b7d0d34586193  
 0x8281aa6795adel7c8973e1aedca380258bc124f9  
 0x57b2b8c82f065de8ef5573f9730fc1449b403c9f  
 0x05e0b5b40b7b66098c2161a5ee11c5740a3a7c45

- d. Seven of the addresses in OFAC's designation are smart contracts that govern additional features of Tornado Cash.<sup>10</sup> Upon information and belief, some were in use at the time they were added to the SDN List, while others were not.
- e. Two of the addresses in OFAC's designation accept donations. One address (0xdd4c48c0b24039969fc16d1cdf626eab821d3384) is a smart contract associated with Gitcoin, a platform where developers are paid to work on open-source software in various programming languages. The other address (0x8589427373D6D84E98730D7795D8f6f8731FDA16) appears to be controlled by a user not identified or designated by OFAC.
- f. One address (0x756c4628e57f7e7f8a459ec2752968360cf4d1aa) is an inalterable smart contract that allows users to input a message of their choice so that the smart contract can echo or repeat that message back to the Ethereum blockchain.

---

0x23173fe8b96a4ad8d2e17fb83ea5dccccdca1ae52  
 0x538ab61e8a9fc1b2f93b3dd9011d662d89be6fe6  
 0x94be88213a387e992dd87de56950a9aef34b9448  
 0x242654336ca2205714071898f67e254eb49acdce  
 0x776198ccf446dfa168347089d7338879273172cf  
 0xedc5d01286f99a066559f60a585406f3878a033e.

<sup>10</sup> Those addresses are as follows:

0x94c92f096437ab9958fc0a37f09348f30389ae79  
 0xd82ed8786d7c69dc7e052f7a542ab047971e73d2  
 0xd692fd2d0b2fbd2e52cfa5b5b9424bc981c30696  
 0xb04e030140b30c27bcdfaafffa98c57d80eda7b4  
 0x2fc93484614a34f26f7970cbb94615ba109bb4bf  
 0x26903a5a198d571422b2b4ea08b56a37cbd68c89  
 0x5cab7692d4e94096462119ab7bf57319726eed2a.

### **THE CONSEQUENCES OF DEFENDANTS' DESIGNATION**

71. When a person is identified on the SDN List, United States persons are generally prohibited, on pain of criminal and civil penalties, from doing business with such persons or engaging in financial transactions in which the designated person has a property interest. This prohibition prevents United States persons, including United States financial institutions, from providing funds, goods, or services to the designated person, including opening or maintaining an account for a designated person or processing transactions involving the designated person. Additionally, United States persons, including United States financial institutions, are required to block any property or interests in property of that designated person, and are required to report any such blocked property in their possession or control to OFAC. *See* 31 C.F.R. § 578.201(a), (b); 31 C.F.R. § 510.201; *see also* 87 Fed. Reg. 54,373 (Sept. 6, 2022) (amending OFAC's Cyber-Related Sanctions Regulations).

72. OFAC has recognized that “most virtual currency activity is licit.” *See U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, OFAC (May 6, 2022) <[home.treasury.gov/news/press-releases/jy0768](https://home.treasury.gov/news/press-releases/jy0768)>.

73. Nevertheless, as a result of the August 8 designation and November 8 redesignation, no Ethereum user subject to United States jurisdiction can lawfully use Tornado Cash for any purpose without fear of serious consequences as a result of government enforcement. Plaintiffs and other law-abiding citizens are prohibited from depositing, withdrawing, sending, or receiving funds through Tornado Cash, even when the funds have no connection to illicit activity.

74. What is more, the open-source, self-executing code is still operational. The fact that no intermediary is necessary means that United States persons with public Ethereum wallet addresses may receive unsolicited crypto assets sent through Tornado Cash.

75. Without an injunction, the designation will prevent Plaintiffs and others who are similarly situated from using Tornado Cash. Because OFAC's designation does not expire, United States persons who had funds in Tornado Cash pools at the time of Tornado Cash's designation are indefinitely prohibited from lawfully accessing those funds. Ethereum users will be forced to choose between transacting without the privacy benefits of Tornado Cash and foregoing the opportunity to engage in potentially valuable personal and business transactions.

76. The ongoing harms are immediately redressable by an injunction. An order to remove Tornado Cash and the Tornado Cash smart contracts from the SDN List would allow Plaintiffs to conduct their legitimate business activities with some measure of anonymity, use their preferred software tool without fear of penalties, and retrieve their locked funds from Tornado Cash.

77. An injunction would also serve the public interest by averting harm to Tornado Cash users who are United States persons, the broader Ethereum network, and the important sector of the economy that depends on the Ethereum network.

78. Defendants' action on November 8, like Defendants' action on August 8, constitutes final agency action.

**COUNT I**  
**(ALL PLAINTIFFS)**

**Administrative Procedure Act**  
**(5 U.S.C. § 706(2)(A), (C))**

79. Plaintiffs incorporate by reference the factual allegations in ¶¶ 1-78.

80. The statutes invoked by Defendants do not authorize their action.

81. Defendants have authority under IEEPA to regulate certain activities involving "any property in which any foreign country or a national thereof has any interest by any person, or with respect to any property, subject to the jurisdiction of the United States." 50 U.S.C. § 1702(a)(1)(B).

82. Defendants have authority under the United Nations Participation Act of 1945 to “investigate, regulate, or prohibit, in whole or in part, economic relations or rail, sea, air, postal, telegraphic, radio, and other means of communication between any foreign country or any national thereof or any person therein and the United States or any person subject to the jurisdiction thereof, or involving any property subject to the jurisdiction of the United States.” 22 U.S.C. § 287c(a).

83. Defendants have authority under the North Korea Sanctions and Policy Enhancement Act of 2016 to designate “any person” engaged in certain conduct relating to North Korea. 22 U.S.C. § 9214.

84. Tornado Cash is not “property,” a “foreign country or a national thereof,” or a “person” of any kind under IEEPA. Tornado Cash is not “property,” a “foreign country or any national thereof,” or a “person” of any kind under the United Nations Participation Act. And Tornado Cash is not a “person” under the North Korea Sanctions and Policy Enhancement Act.

85. The Tornado Cash smart contracts are not “property,” a “foreign country or a national thereof,” or a “person” of any kind under IEEPA. The Tornado Cash smart contracts are not “property,” a “foreign country or any national thereof,” or a “person” of any kind under the United Nations Participation Act. The Tornado Cash smart contracts are not a “person” under the North Korea Sanctions and Policy Enhancement Act. And the Tornado Cash smart contracts are not identifiers for any of the above.

86. Defendants’ designation is therefore “not in accordance with law” and is “in excess of statutory jurisdiction, authority, or limitations” under the APA. 5 U.S.C. § 706(2)(A), (C).



**COUNT II**  
**(ALL PLAINTIFFS)**

**First Amendment to the United States Constitution and Administrative Procedure Act  
(Freedom of Speech)  
(5 U.S.C. § 706(2)(A), (B))**

87. Plaintiffs incorporate by reference the factual allegations in ¶¶ 1-86.

88. Defendants’ action prohibits Plaintiffs from engaging in speech protected by the First Amendment to the Constitution. By providing a certain degree of privacy, Tornado Cash allows Plaintiffs to engage in important, socially valuable speech. As a result of the designation, Plaintiffs are unable to use Tornado Cash to make donations to support important, and potentially controversial, political and social causes. Plaintiffs are also unable to develop code related to Tornado Cash to facilitate improved uses of Tornado Cash and the Ethereum network. And Plaintiffs are unable to use Tornado Cash to develop future business ventures, which themselves will engage in socially valuable speech.

89. Defendants’ action also prohibits many others from engaging in similarly important, valuable, protected speech. That speech includes donations to important, and potentially controversial, political and social matters; software code; and speech in connection with commercial activities funded by crypto assets sent through Tornado Cash. Because Tornado Cash is frequently used for those lawful purposes, Defendants’ action “prohibits a substantial amount of protected speech . . . relative to the . . . plainly legitimate sweep” of Defendants’ action. *United States v. Williams*, 553 U.S. 285, 292 (2008).

90. For all of those reasons, Defendants’ designation is “not in accordance with law” and “contrary to constitutional right” under the APA. 5 U.S.C. § 706(2)(A), (B).

**COUNT III**  
**(PLAINTIFFS TYLER ALMEIDA, PRESTON VAN LOON, AND NATE WELCH)**

**Fifth Amendment to the United States Constitution and Administrative Procedure Act  
(Due Process)  
(5 U.S.C. § 706(2)(A), (B))**

91. Plaintiffs incorporate by reference the factual allegations in ¶¶ 1-90.

92. As a result of Defendants’ action, Plaintiffs Tyler Almeida, Preston Van Loon, and Nate Welch are unable to access Ether that belongs to them because it is trapped in a Tornado Cash pool. That Ether is their property.

93. Mr. Almeida, Mr. Van Loon, and Mr. Welch did not receive any process prior to that deprivation of their property, let alone due process of law.

94. The denial of any pre-deprivation process whatsoever is unjustified by any national security interests, and the risk of erroneous deprivation of property from Defendants’ action is intolerably high under the Fifth Amendment to the U.S. Constitution.

95. Defendants’ designation is therefore “not in accordance with law” and “contrary to constitutional right” under the APA. 5 U.S.C. § 706(2)(A), (B).

**PRAYER FOR RELIEF**

Plaintiffs respectfully pray that this Court enter an order and judgment:

1. Declaring that Defendants’ designation is null, void, and with no force and effect;
2. Declaring that Defendants’ designation is not in accordance with law within the meaning of 5 U.S.C. § 706(2)(A); contrary to constitutional right within the meaning of 5 U.S.C. § 706(2)(B); and in excess of statutory jurisdiction, authority, or limitations within the meaning of 5 U.S.C. § 706(2)(C);
3. Vacating and setting aside the designation;

4. Permanently enjoining Defendants and their officers, employees, and agents from enforcing, implementing, applying, or taking any action whatsoever under, or in reliance on, the designation;

5. Awarding Plaintiffs the costs of this litigation, including reasonable attorney's fees; and

6. Such other and further relief as this Court may deem just and proper.

Dated: November 22, 2022

PAUL, WEISS, RIFKIND,  
WHARTON & GARRISON LLP

Kannon K. Shanmugam\*  
Brian M. Lipshutz\*  
Matteo Godi\*  
Jennifer K. Corcoran\*  
2001 K Street, N.W.  
Washington, DC 20006  
(202) 223-7300 (telephone)  
kshanmugam@paulweiss.com

PARKER, BUNT & AINSWORTH, P.C.

By: /s/ Charles Lewis Ainsworth

Charles Lewis Ainsworth  
Texas Bar No. 00783521  
100 E. Ferguson Suite 418  
Tyler, TX 75702  
(903) 531-3535 (telephone)  
charley@pbatyler.com

\* *Admitted pro hac vice*

**CERTIFICATE OF SERVICE**

I hereby certify that I have served, via CM/ECF, a true and correct copy of the foregoing Amended Complaint upon each attorney of record and the Clerk of the Court on this 22nd day of November, 2022.

By: /s/ Charles Lewis Ainsworth  
Charles Lewis Ainsworth  
Texas Bar No. 00783521