**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF FLORIDA
PENSACOLA DIVISION**

COIN CENTER; PATRICK O'SULLIVAN; JOHN DOE; and DAVID HOFFMAN,	)))	
Plaintiffs,	)))	
v.	))	No. 3:22-cv-20375-TKW-ZCB
JANET YELLEN, in her Official Capacity as Secretary of the Treasury; DEPARTMENT OF THE TREASURY; ANDREW M. GACKI, in her Official Capacity as Director of the Office of Foreign Assets Control; and OFFICE OF FOREIGN ASSETS CONTROL,	))))))))	
Defendants.	)	

**BRIEF OF AMICUS CURIAE PARADIGM OPERATIONS LP
IN SUPPORT OF PLAINTIFFS'
MOTION FOR SUMMARY JUDGMENT**

CORPORATE DISCLOSURE STATEMENT

Paradigm Operations LP ("Paradigm") discloses the following information for the limited purpose of complying with Rule 7.1(a)(1) of the Federal Rules of Civil Procedure. Paradigm has no parent corporation. No publicly held corporation owns 10% or more of Paradigm's stock.

Paradigm reserves the right to supplement this disclosure statement if needed.

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

INTEREST OF AMICUS CURIAE

Paradigm Operations LP ("Paradigm") is an investment firm that backs entrepreneurs building innovative crypto companies and protocols. Paradigm seeks leave to participate in this case because it is concerned that the Department of Treasury's ("the Department") unprecedented sanctioning of publicly available software is an unfounded expansion of sanctions law that exceeds the Department's statutory authority and would deprive law-abiding Americans of a critical privacy tool. Moreover, the novel argument the Department puts forward to justify its regulation of technology—essentially that developers and users of Tornado Cash form some sort of unincorporated entity that holds a property interest in immutable open source software—is itself a broad and far-reaching theory that would effectively conscript unwitting coders and technology users into becoming members of a legal entity not of their choosing and, as a result, inhibit the viability of open-source software development in the United States.

INTRODUCTION

Blockchain technology is an emerging computing paradigm that, while still in its early stages of development, has made peer-to-peer digital payments possible and is enabling new forms of human coordination and more complex applications that are colloquially referred to as "Web3." Blockchains are at their core computer networks that enable a decentralized set of unaffiliated "nodes" to maintain a shared database. One of blockchain technology's defining features is that this shared database or "ledger" is completely transparent: anyone can view all of the information dating back to the first transaction.

A blockchain's transparency provides an important safety measure since it allows anyone to audit the data. However, it can also raise alarming privacy concerns for users. While a blockchain user's address is pseudonymous, if linked to a real-world identity (which happens), it

could expose that user's complete history, including sensitive transactions or affiliations, and make them the target of bad actors. In practice, this is akin to publishing one's entire history of bank account statements or credit card bills for anyone to see online. Moreover, as blockchain adoption increases and more users rely on blockchain infrastructure for online financial and social interactions, these privacy concerns will only increase.

Tornado Cash is a publicly available software, a tool or application, that was designed to address these privacy concerns and enable Ethereum users to shield their information. The core Tornado Cash tools are "pools," which refer to applications enabled by smart contracts deployed to the Ethereum blockchain that allow users to deposit tokens from one address and later withdraw those same tokens to a different address on the Ethereum network.[1] While a user's deposit or withdrawal from a Tornado Cash pool is publicly broadcast on the Ethereum network, the link between the deposit and withdrawal addresses is broken. Tornado Cash, therefore, acts as a type of "private changing room" that provides the withdrawal address with some level of privacy because it cannot easily be linked to the deposit address. The level of privacy increases as the relevant pool has more volume.

The smart contracts for the relevant Tornado Cash pools are "immutable"—that is, no one can control, update, or remove them from the Ethereum network. In addition, Tornado Cash pools

---

[1] "When developers program smart contracts, they decide what operations the smart contract will support and what rules those operations must follow. These rules and operations are written using code that is broadcast to Ethereum's network, just like the token transactions described above. Once a smart contract's code is added to Ethereum's records, it receives a unique address and can be interacted with by any user to automatically carry out the rules and operations it supports. In essence, smart contracts are open-source applications that anyone can deploy to Ethereum. Just like the rest of Ethereum, smart contracts can be viewed and used by anyone, anywhere, and without relying on an intermediary." Alex Wade, Michael Lewellen & Peter Van Valkenburgh, *How does Tornado Cash Work?* Coincenter (Aug. 25, 2022), https://bit.ly/3KZwBUy.

are entirely "non-custodial," meaning that a user who deposits tokens into the pool is never required to relinquish control of those tokens.

When Tornado Cash is properly conceptualized as an array of publicly available software applications—*i.e.*, code—that cannot be owned, updated, or removed and that do not take control of users' assets, it is clear that "Tornado Cash" is not a legal person that should be subject to sanctions.[2] However, in a gambit to expand its authority to regulate technology, the Department argues that "Tornado Cash" is an undefined type of "entity." *Treasury Designates DPRK Weapons Representatives*, U.S. Dep't of Treasury (Nov. 8, 2022), https://bit.ly/3UORTHP. But in fact, Tornado Cash is just open-source code:

```
/**
 *Submitted for verification at Etherscan.io on 2019-12-16
 */

// File: contracts/MerkleTreeWithHistory.sol

// https://tornado.cash
/*
* d888888P                                          dP        a88888b.              dP
*    88                                             88       d8'  '88              88
*    88    .d8888b. 88d888b. 88d888b. .d8888b. .d888b88 .d8888b.    88        .d8888b. .d8888b. 88d888b.
*    88    88'  '88 88'  '88 88'  '88 88'  '88 88'  '88 '88        88        88'  '88 Y8ooooo. 88'  '88
*    88    88.  .88 88       88       88 88.  .88 88.  .88 dP Y8.    .88 88.  .88    88 88    88
*    dP    '88888P' dP       dP       dP '88888P8 '88888P8 '88888P' 88  Y88888P' '88888P8 '88888P' dP    dP
* oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo
*/

pragma solidity ^0.5.8;

library Hasher {
  function MiMCSponge(uint256 in_xL, uint256 in_xR) public pure returns (uint256 xL, uint256 xR);
}


contract MerkleTreeWithHistory {
  uint256 public constant FIELD_SIZE =
21888242871839275222246405745257275088548364400416034343698204186575808495617;
  uint256 public constant ZERO_VALUE =
21663839004416932945382355908790599225266501822907911457504978515578255421292; // = keccak256("tornado") %
FIELD_SIZE
```

---

[2] There are centralized businesses that offer "mixing" services, such Blender.io, which have also been the subject of sanctions by the Department. *U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats*, U.S. Dep't of Treasury (May 6, 2022), https://bit.ly/41rOCQI. In stark contrast to Tornado Cash, mixers like Blender.io work by requiring users to relinquish their tokens to a centralized business entity, which will exercise control over those tokens and subsequently return them to the user for a fee.

Tornado Cash Contract Source Code, Etherscan, https://bit.ly/41fprkz. The Department therefore

has no authority to sanction Tornado Cash, and this Court should grant the Plaintiffs' Motion for

Summary Judgment.

ARGUMENT

I.   The Department's authority is limited to blocking "property" of "persons."

The Department sanctioned Tornado Cash pursuant to Executive Orders (E.O.) 13694 and

13722. Broadly, E.O. 13694 issued by President Barack Obama in April 2015 "block[s]" and

prohibits the transfer or dealing of "[a]ll property and interests in property" of "any person" the

Department has determined to have engaged in "significant malicious cyber-enabled activities."

E.O. No. 13694, 80 Fed. Reg. 18,077 (Apr. 1, 2015). E.O. 13722, issued by President Obama in

March 2016, "block[s]" and prohibits the transfer or dealing of "[a]ll property and interests in

property" of the North Korean government within the United States or in the control of a United

States person or of "any person" who generally conducts or has conducted business with the North

Korean government. E.O. No. 13722, 81 Fed. Reg. 14,943 (Mar. 15, 2016). Each E.O. applies only

to "property" or "interests in property" "that are in the United States, that hereafter come within

the United States, or that are or hereafter come within the possession or control of any United

States person." E.O. 13694; E.O. 13722.

Of course, "an agency literally has no power to act . . . unless and until Congress confers

power upon it." *Louisiana Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986). Both E.O.s

13694 and 13722 were issued, in part, pursuant to the International Emergency Economic Powers

Act (IEEPA), which permits the President "under such regulations as he may prescribe" to:

> 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)(B). E.O. 13722 was also issued, in part, pursuant to the North Korea Sanctions and Policy Enhancement Act of 2016, which permits the president to "designate . . . any person" the President determines has knowingly assisted or engaged in commerce with the North Korean government. 22 U.S.C. § 9214(a).

The Department's own regulations clearly define "person," "property," and "interest." In brief, "property" and "property interest" are assets, tangible or intangible, that are capable of being owned. *See* 31 C.F.R. § 510.323. And under the Department's designation and regulations, a "person" includes an "individual or entity," with an entity defined as "a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization." 31 C.F.R. §§ 510.322; 510.305. Although IEEPA, the Department's own regulations, and the E.O.s do not further define "a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization," *id.*, dictionary definitions confirm that an "entity" generally means a group of individuals that intend to work toward a common purpose.[3]

---

[3] **Partnership**: "A voluntary association of two or more persons who jointly own and carry on a business for profit." Black's Law Dictionary (11th ed. 2019).
Association: "A gathering of people for a common purpose; the persons so joined." *Id*.
Joint Venture: "A business undertaking by two or more persons engaged in a single defined project. The necessary elements are (1) an express or implied agreement; (2) a common purpose that the group intends to carry out; (3) shared profits and losses; and (4) each member's equal voice in controlling the project." *Id*.
Corporation: "An entity (usu. a business) having authority under law to act as a single person distinct from the shareholders who own it and having rights to issue stock and exist indefinitely; a group or succession of persons established in accordance with legal rules into a legal or juristic person that has a legal personality distinct from the natural persons who make it up, exists indefinitely apart from them, and has the legal powers that its constitution gives it." *Id*.
Group: "A number of individuals assembled together or having some unifying relationship." Merriam-Webster (2023), bit.ly/3IPf4N1.

Accordingly, for parties to form an entity that can be the subject of legal action, there must be an *intent* to work toward a common purpose. Indeed, courts impose that requirement in a variety of statutory contexts where defining "the outer boundaries" of "entity" is necessary. *See, e.g.*, *Boyle v. United States*, 556 U.S. 938, 944 (2009) (explaining, in the RICO context, that the statute covers any "group of persons associated together for a common purpose of engaging in a course of conduct" (citation omitted)); *Dole v. Odd Fellows Home Endowment Bd.*, 912 F.2d 689, 692 (4th Cir. 1990) (holding that, for "entities" to form an "enterprise" subject to the Fair Labor Standards Act, they must share "a common business purpose"); *Al-Rayes v. Willingham*, 914 F.3d 1302, 1308 (11th Cir. 2019) ("[T]he concept of 'associat[ion]' requires both interpersonal relationships and a common interest." (citation and internal quotation marks omitted)).

This requirement makes good sense. The existence of a "common purpose" is necessary to "identify[] and defin[e] the enterprise." *Kruse by & through Kruse v. Repp*, 543 F. Supp. 3d 654, 680 (S.D. Iowa 2021). Without the "limiting principle of a shared common purpose among members," any group of individuals could be cast as an entity susceptible to sanction. *United States v. Cianci*, 378 F.3d 71, 88 (1st Cir. 2004). After all, with enough thought, commonalities can be identified between any group of individuals. Thus, to prevent a "potentially boundless" definition, only groups of individuals that *intend* to work toward some common goal qualify as an "entity" susceptible to sanction. *See Ryan v. Clemente*, 901 F.2d 177, 180 (1st Cir. 1990).

II.   Tornado Cash is not a person or entity that the Department has authority to sanction, and it does not own property or have property interests.

Here, however, the Department has been unable to identify a shared common purpose or, indeed, any limiting principle to define the "entity" it is sanctioning. There is no evidence that

---

Organization: "A group that has formed for a particular purpose." Black's Law Dictionary (11th ed. 2019).

Tornado Cash, its founders, associated developers, or the diffuse number of individuals holding Tornado Cash "TORN" digital tokens have ever intended to work toward a common purpose. Even if Tornado Cash were the kind of "entity" the Department has statutory authority to sanction, the immutable, open-source contracts it sanctioned are not property of Tornado Cash. The Department therefore exceeded its statutory authority.

A. Tornado Cash is not a person or entity that can be sanctioned.

Tornado Cash is a software program. Yet at various stages, the Department has stated that the "person" it has sanctioned is "the entity known as Tornado Cash, which is a 'partnership, association, joint venture, corporation, group, subgroup, or other organization.'" *Cyber-Related Sanctions, FAQ 1095*, Office of Foreign Asset Control, (Nov. 8, 2022), https://bit.ly/3KMRx0C ["FAQ 1095"]. Notably, the Department has not specified which *type* of entity Tornado Cash is, opting instead to simply refer to the full regulatory definition of "entity." 31 C.F.R. §§ 510.305, 578.305.

The Department's theory for sanctioning Tornado Cash is that Tornado Cash is a Frankenstein-like creature, assembled from disparate components that, when combined, become a legal person. Peter Van Valkenburgh, *Tornado Cash is No "Golem." It's a Tool for Privacy and Free Speech*, CoinCenter (Oct. 26, 2022), https://bit.ly/3o8lZJL. According to the Department, the Tornado Cash "organizational structure" consists of: (1) unnamed "founders and other associated developers" and (2) "the Tornado Cash [Decentralized Autonomous Organization] DAO. . . ." FAQ 1095.[4]

---

[4] Fundamentally, DAOs are a way to organize people, a social-coordination technology that relies on blockchain-based smart contracts and incentives to facilitate individuals collaborating and taking actions with collective impact. DAOs enable increased "transparency, trust, adaptability and speed" in making decisions as compared to traditional decision-making approaches. David

But the Department cannot identify any limiting principle to its theory. Nothing in the record suggests that Tornado Cash's founders and associated developers have intended to work toward a common purpose, nor do they have any power or control over the immutable Tornado Cash pools or one another. Tornado Cash is best defined as a "tool" or "software." Valkenburgh, *supra*. Like any online tool, it can be used "for illegal—and sometimes terrible—ends," but the "mere creation of [a] platform" does not establish a common purpose, much less intent to engage in unlawful activity. *Twitter v. Taamneh*, No. 21-1496, 598 U.S. ___ (2023), slip op. at 23 (May 18, 2023).

The publicly available Tornado Cash codebase has 11 individual contributors, including presumably some of the unnamed founders. *Tornadocash*, Github, https://bit.ly/3o9FmlO. But the Tornado Cash code builds upon existing open-source code and incorporates dependencies[5] that themselves are the product of contributions from many thousands of unaffiliated developers over many years. Read literally, the Department's statement that Tornado Cash is an unincorporated entity partially made up of "founders and associated developers" could be interpreted to encompass even developers that have only contributed code indirectly. FAQ 1095. The Department has not delineated exactly which of these contributors are supposedly part of the undefined association, nor has it shown they have intended to work toward a common purpose. This Court should make clear that developers do not get conscripted into a legal entity when they suggest a revision to publicly available code, or have their existing code integrated into a new codebase.

Gogel et al., *Decentralized Autonomous Organizations: Beyond the Hype*, World Econ. F., 4–5 (June 2022), https://bit.ly/3KvLFaU.

[5] In the context of software development, a "dependency" is a relationship between software components where one component relies on the other to work properly. For example, if a software application uses a library to query a database, the application depends on that library.

The Department argues the second component of the Tornado Cash entity is the Tornado Cash DAO. The DAO includes thousands of holders of digital tokens known as "TORN." *Tornado Cash*, CoinMarketCap, https://bit.ly/3KMr6YZ. The TORN holders acquired the token for different reasons and have potentially conflicting motivations and incentives. Some TORN holders may vote on certain governance related proposals created by developers. They do not, however, have any control over the Tornado Cash pools.

The Department's novel theory that Tornado Cash is an entity because it consists of unnamed founders, associated developers, and TORN token holders fails because this disparate mix of actors have wide ranging levels of involvement in the project, including no involvement at all. As a result, they collectively lack the level of coordination needed to be considered a unified legal entity. For the same reason, the Tornado Cash DAO is not an entity working towards a common purpose. Merely voting on proposals does not mean that TORN token holders have intended to work toward a common purpose, and it is not enough to create an unincorporated association.

In addition, the Department's description of TORN token holders is inaccurate. Token holders are not "responsible" for voting, *contra* FAQ 1095, which is completely voluntary and in practice has extremely low participation. A person can purchase tokens, simply hold them, and never choose to vote on anything. Alternatively, a TORN holder may participate in one vote and then sell tokens without interacting with Tornado Cash again or delegate voting rights to others. More importantly, token holders are not "voting on and implementing new features" as they relate to the core Tornado Cash privacy tool because the Tornado Cash smart contract "pools" are all immutable, and so TORN token holders have no power to change them.

9

There is no dispute that the Department *can*, in some circumstances, sanction entities that use blockchain technology. *See* Nikhilesh De, *Crypto Exchange Poloniex Agrees to $7.6M Fee to Settle Sanctions Violation Charges*, CoinDesk (May 2, 2023), bit.ly/3WryTQk; *OFAC Sanctions Hydra Following Law Enforcement Shutdown of the Darknet Market, As Well As Russian Exchange Garantex*, ChainAnalysis (April 5, 2022), bit.ly/3MSgR6H. For example, the Department has also sanctioned Blender.io, and that "announcement drew no objection from the cryptocurrency community." Jerry Brito & Peter Van Valkenbough, *Analysis: What is and What is Not a Sanctionable Entity in the Tornado Cash Case*, Coin Center (August 15, 2022), bit.ly/432ctaS. That is because Blender is a definable "entity that is ultimately under the control of certain individuals." *Id.* Thus, the problem is not that Tornado Cash involves decentralized blockchain governance nor that some of its developers are anonymous. Instead, the problem is the Department's attempt to sanction an unspecified entity of entirely undefined scope.

The Department cannot answer fundamental questions about what and who it is sanctioning. This is not a scenario, as the Department has tried to contend, where the entity being sanctioned is clearly defined, even if some members of the entity might be unknown (like Al Qaeda, for instance). The Department has not and cannot identify the core, defining features of the entity it is sanctioning. How "associated" must a developer be to be part of Tornado Cash? FAQ 1095 offers no answer. Most of the constituent members of the DAO never interact with Tornado Cash—are they still part of an entity working towards some identified purpose? These central ambiguities are confirmation that the Department is not in fact sanctioning an entity at all.

B. Tornado Cash does not own or have an interest in smart contracts.

Because Tornado Cash is a software tool, not an entity, it cannot own "property" or have a "property interest." 31 C.F.R. § 510.323. And even assuming there was some kind of distinct "Tornado Cash Entity," it would "not have a property interest in the Tornado Cash" smart

10

contracts. Brito, et al., *supra*. These publicly available immutable smart contracts, based on open-source software, cannot be controlled or owned.

"Tornado Cash," at is core, is "synonymous" with "the Tornado Cash smart contracts." Wade, et al., *supra*. "The vast majority of these" existing smart contracts, including each of the pool contracts, "are immutable. That is, they have no ability to be updated or removed by anyone." *Id.* Indeed, these "smart contracts" are "non-proprietary software residing simultaneously on the computers of every person around the world running the Ethereum open source client." Brito, et al., *supra*. In fact, because the code for these contracts is open source, "anyone can deploy [them] to Ethereum." Wade, et al., *supra*. And once deployed, these contracts can be set so that they are immutable. Proving the point, even though a malicious actor recently gained control of Tornado Cash's governance structure, the smart contracts governing the pools (and coins within them) remained uncompromised. *See* Arijit Sarkar, *Tornado Cash Attacker to Potentially Give Back Governance Control, Proposal Reveals*, CoinTelegraph (May 22, 2023), bit.ly/3MYLuHD. Because no one has any "legal right" or "ability to control" these smart contracts, and because this open-source code can be deployed by anyone, this software "is not even 'property' in any reasonable sense of the word." Brito, et al., *supra*.

To help clarify why this is so, consider the Department's sanctions levied against Blender.io. Blender offers cryptocurrency mixing services. *Id.* But unlike Tornado Cash smart contracts, Blender works by "tak[ing] control of th[e] coins," mixing "your coins with those of other customers," and then "send[ing] an equivalent amount back to you minus a fee." *Id.* In other words, Blender is a definable entity with control over property (the coins) that can choose whether and with whom to transact. The undefined, theoretical "Tornado Cash Entity," by contrast, never

11

takes custody of coins and has no control over whether a person uses an existing smart contract. *Id.* Because these smart contracts cannot be owned or controlled, they are not property.

Nor does the use of the pool smart contracts produce any financial benefit for "Tornado Cash," however defined. When a user deposits or withdraws tokens from a pool, no Tornado Cash entity (assuming again, one even exists—it does not) is a party to that transaction or otherwise receives anything of value. *See* Wade, et al., *supra*. It is true that some Tornado Cash users take advantage of "an optional service" involving "independent operators," called "relayers." *Id.* Relayers help "users maintain privacy when withdrawing" coins from a pool by acting as a middle-man that pays the transaction cost required to send the coins to the withdrawal address, "earning a fee in the process." *Id.* And some relayers pass a portion of that fee on to a treasury for the Tornado Cash DAO. But using those relayers is not required, as the chart below shows. Anyone, including Paradigm, could run a relayer by deploying the publicly available open-source code. *Tornadocash/Tornado-Relayer*, GitHub, bit.ly/3WPAL5G.
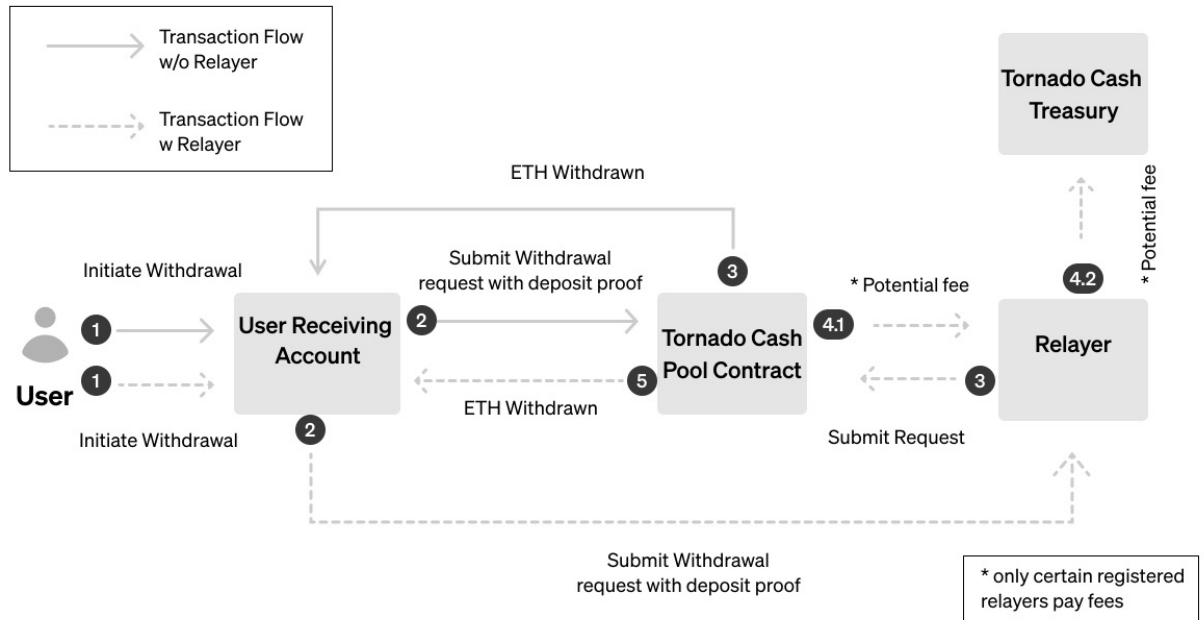
The Plaintiffs in this case do not intend to use the relayers that make payments to the DAO, and the use of those relayers would remain illegal if the Plaintiffs prevailed. Docs. 36-2, 36-3, 36-4, 36-5; Doc. 9 at 40-44. The Plaintiffs and other Tornado Cash users can use the pool smart contracts without any relayers or can use relayers that are set up by an independent party like Paradigm that do not pay any fees to the DAO treasury. The DAO cannot have a property interest in transactions that it will not receive anything from.

III.   The Department's theory for sanctioning Tornado Cash is unprecedented and far-reaching.

The Department's theory for sanctioning Tornado Cash implies that unassociated developers can become part of an "entity" simply because they have contributed code, knowingly or unknowingly, to a blockchain protocol. Blockchain-enabled communities, in particular DAOs, have taken shape in ways that do not conform to existing corporate entities, such as corporations or limited liability companies. *Cf.* Chris Brummer and Rodrigo Seira, *Legal Wrappers and DAOs* (July 7, 2022), https://bit.ly/43vD8xi. As a result of the mismatch between blockchain-enabled communities and recognized legal entities, the potential liability of various participants in these communities is an open question that is being litigated in various regulatory and civil actions. The Department's theory for sanctioning Tornado Cash here is fundamentally that disparate unaffiliated individuals can form an unincorporated entity capable of being sanctioned, which implies that the Department could, if it wanted, go after code developers who have contributed to open-source publicly available codes like Tornado Cash merely because of their contribution to that code.

This is a slippery slope—implying that code developers can unwittingly be roped into sanctions through their code contributions. And it goes beyond the liability theories other agencies have relied upon. For instance, in the first regulatory enforcement action involving a DAO, the

Commodity Futures Trading Commission (CFTC) merely argued that the "Ooki DAO"—another blockchain protocol—was an unincorporated general partnership comprised of token holders who actually voted. *See Commodity Futures Trading Comm'n v. Ooki DAO*, No. 3:22-CV-05416-WHO, 2022 WL 17822445, at *8 (N.D. Cal. Dec. 20, 2022) (holding that the Ooki DAO was capable of being served, but deferring the question whether it was "an association that can be held liable" under the Commodity Exchange Act). Although the CFTC's position that this DAO is an unincorporated general partnership is wrong, the Department's position in this case goes even further—implying that *all* TORN token holders *plus* Tornado Cash's founders and associated developers can form an unincorporated entity.

Moreover, the Department's attempt to conscript developers and token holders into joining a Frankenstein unincorporated association could imperil the viability of open-source code development in the United States. Open-source code is the backbone of today's technological stack, and the product of countless contributions from individual developers. As an indirect result of this case, these developers could suddenly find themselves at risk of being unwittingly ensnared into joining a legal entity by simply making contributions to open-source code. Indeed, the lack of clarity about what specific test the Department used to determine organizational status and membership is so unclear that it would be difficult for people to know for sure if their activities— which might be as simple as receiving a TORN token unwittingly from another and leaving it in their wallet—could subject them to being considered members of an unincorporated association with devastating legal consequences. Or, consider a developer whose unrelated open-source software contribution to the public domain was used in code development. Could that unknowing contribution trigger membership in an unincorporated association and thus subject him to sanctions?

14

To avoid inhibiting Americans from freely contributing to the development of publicly available technologies, this Court should be extremely weary of endorsing the Department's theories about the presumed collective legal personhood of individuals interacting with software.

*   *   *

Essentially, the Department's sanctioning here is a ban on privacy technology like Tornado Cash. Yet there are important, non-nefarious reasons why law-abiding citizens seek to use Tornado Cash to protect their transactions. Today, you can use digital currency for mundane day-to-day transactions like buying a movie ticket or for transactions that reasonable people would want to keep private—paying for a doctor's visit or donating to political or charitable causes. As digital currencies like Ethereum become more established, protecting this privacy will become even more important. After all, the current default is that financial transactions are generally private, and no one expects to see their credit or debit card transactions posted publicly for the world to see and traced back to them. There is no reason why Ethereum users should not be able to avail themselves of the same level of protection and anonymity in their transactions through the use of applications like Tornado Cash. And the Department's unparalleled and expansive use of its authority not only represents a real threat to financial privacy but also to the future of open-source code development and the digital blockchain industry more generally.

CONCLUSION

The Court should grant Plaintiffs' motion for summary judgment.

Dated: June 2, 2023

Respectfully submitted,

/s/ Katherine C. Yarger
Katherine C. Yarger*
katie@lkcfirm.com
LEHOTSKY KELLER COHN LLP
700 Colorado Blvd., #407
Denver, CO 80206

15

(512) 693-8350

Rodrigo Seira**
rodrigo@paradigm.xyz
PARADIGM OPERATIONS LP
548 Market Street
San Francisco, CA 94104

*Pro Hac Vice
**Pro Hac Vice Pending

16

CERTIFICATE OF SERVICE

I hereby certify that on June 2, 2023, I electronically filed the foregoing with the Clerk of

Court using the CM/ECF system, which will send a notice of electronic filing to all counsel of

record who have consented to electronic notification.

/s/ Katherine C. Yarger
Katherine C. Yarger

17