No. 23-50669

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIFTH CIRCUIT

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

Plaintiffs-Appellants,

v.

DEPARTMENT OF THE TREASURY, OFFICE OF FOREIGN ASSETS CONTROL, JANET YELLEN, U.S. SECRETARY OF TREASURY, IN HER OFFICIAL CAPACITY, AND ANDREA M. GACKI, IN HER OFFICIAL CAPACITY AS DIRECTOR OF THE OFFICE OF FOREIGN ASSETS CONTROL

Defendants-Appellees.

On Appeal from the United States District Court
for the Western District of Texas
Civil Action No. 1:23-cv-00312-RP

BRIEF FOR *AMICUS CURIAE* BLOCKCHAIN ASSOCIATION
IN SUPPORT OF PLAINTIFFS-APPELLANTS

Eric Tung
JONES DAY
555 South Flower Street,
Fiftieth Floor
Los Angeles, CA 90071
(213) 489-3939

Mark R. Rasmussen
JONES DAY
2727 North Harwood Street
Suite 500
Dallas, TX 75201
(214) 220-3939
mrasmussen@jonesday.com

Alexis Zhang
JONES DAY
51 Louisiana Avenue, N.W.
Washington, DC 20001
(202) 879-3939

Counsel for Amicus Curiae

SUPPLEMENTAL STATEMENT OF INTERESTED PARTIES

Pursuant to Fifth Circuit Rule 29.2, I hereby certify that the following persons and entities have an interest in the outcome of the case under Rule 28.2. These representations are made so that judges may evaluate potential recusal.

1) *Amicus Curiae*: Blockchain Association

2) Counsel for *Amicus Curiae*: Mark W. Rasmussen, Eric Tung, and Alexis Zhang, Jones Day

11) Disclosure Statement: The Blockchain Association is a nonprofit organization organized under the laws of the District of Columbia. It has no parent corporation, and no publicly held company owns ten percent or more of its stock.

/s/ Mark W. Rasmussen
Mark W. Rasmussen

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

INTEREST OF *AMICUS CURIAE*[1]

Amicus curiae, the Blockchain Association, is the leading nonprofit membership organization dedicated to promoting a pro-innovation policy environment for digital assets. *Amicus* endeavors to achieve regulatory clarity and to educate policymakers, regulators, courts, and the public about how blockchain technology can pave the way for a more secure, competitive, and consumer-friendly digital marketplace. It represents more than 100 member companies that reflect the diversity of the dynamic blockchain industry, including software developers, infrastructure providers, exchanges, custodians, investors, and others supporting the public blockchain ecosystem.

The Office of Foreign Assets Control (OFAC) decision to sanction Tornado Cash—privacy-protecting software used on the Ethereum blockchain—raises serious regulatory and constitutional questions with important implications for the blockchain ecosystem and the digital asset economy. *Amicus* submits this brief to assist the Court in understanding

---

[1] No counsel for any party authored this brief in whole or in part and no entity or person, apart from *amicus curiae*, its members, or its counsel, made any monetary contribution intended to fund the preparation or submission of this brief. *See* Fed. R. App. P. 29(a)(4)(E). All parties have consented to the filing of this brief.

blockchain technology and the serious legal problems posed by the Tornado Cash sanctions.

INTRODUCTION AND SUMMARY OF ARGUMENT

In upholding the Office of Foreign Assets Control's sanctions of Tornado Cash, the District Court repeated OFAC's mistakes—misunderstanding what Tornado Cash is and overestimating the breadth of OFAC's sanctioning authority. OFAC's authorizing statutes permit it to block access to Tornado Cash—self-executing computer software available on the Ethereum blockchain—only if Tornado Cash is property in which a sanctioned foreign person has a cognizable interest.[2] But Tornado Cash is not property belonging to any person, and regardless there is no Tornado Cash "person" within the meaning of OFAC's authorizing statutes.

As a result, Americans continue to be wrongly denied access to what was previously the most popular privacy-protecting tool on Ethereum, the world's second-largest public blockchain.[3] And Tornado Cash is just

---

[2] Throughout this brief, *amicus* uses "Tornado Cash" as a shorthand for the immutable smart contracts sanctioned by OFAC.

[3] *See* George Kaloudis & Edward Oosterbaan, *How Popular Are Crypto Mixers? Here's What the Data Tells Us*, CoinDesk (Nov. 7, 2022),

that—an autonomous tool. This software has no owner or operator, and it functions automatically without any human intervention or assistance. Like any tool—indeed, like the internet itself—software like Tornado Cash can be misused for illicit purposes. But it is used primarily for legitimate and socially valuable reasons. *See* Appellants' Br. 38–39.

As free-standing software, the Tornado Cash computer code cannot be sanctioned under the statutes that OFAC has invoked. To the extent this leaves OFAC disempowered, the proper remedy is to seek legislation from Congress that would provide supplemental authority in the uniquely decentralized digital asset context—not to improperly stretch its existing authorities. Such a power-grab would be a slippery slope that could threaten all manner of internet-based tools that have heretofore been freely available. This Court should reverse the District Court's grant of summary judgment to OFAC and direct judgment for the Plaintiffs.

---

https://bit.ly/3Xb0iok; *Today's Cryptocurrency Prices by Market Cap*, CoinMarketCap, https://bit.ly/3IFcoSs (last visited Nov. 19, 2023).

ARGUMENT

I.   TORNADO CASH IS AN IMPORTANT TOOL FOR PROTECTING THE PRIVACY OF DIGITAL ASSET USERS.

Americans today use digital assets more than ever. A recent study found that 20 percent of American adults own digital assets, and 29 percent plan to buy or trade digital assets in the next year.[4] And it is not hard to see why: public blockchain networks utilize blockchain technology as a decentralized, internet-based alternative to perform the communication and settlement functions necessary for transfers of data, thus freeing users from the multitude of third-party middlemen familiar to traditional finance, like banks and payment processors, and even from fiat currencies.[5]   This freedom is not only more efficient and less expensive than legacy systems, but it also allows users to regain the power and ownership taken away from them by intermediaries.[6] In doing

---

[4] *Cryptocurrency Perception Study*, Morning Consult (Feb. 24, 2023), https://bit.ly/3FUayeO.

[5] *See generally What Is Cryptocurrency?*, Coinbase, https://bit.ly/3lSamp7 (last visited Nov. 19, 2023).

[6] *See, e.g.*, Jerry Brito, *Report: The Case for Electronic Cash*, Coin Center (Feb. 2019), https://bit.ly/3Z2ybcj; Aaron Terr, *PayPal Is No Pal to Free Expression*, Found. for Individual Rts. & Expression (Sept. 30, 2022), https://bit.ly/3Z0pKOw.

so, it creates a valuable alternative for the millions of Americans who are "unbanked" or "underbanked" by the world's historically discriminatory and increasingly powerful traditional financial institutions.[7]

In considering the application of this emerging technology to this appeal, two points are critical. *First*, as detailed below, people conduct digital asset transactions through a public "blockchain," which is an interconnected network of computers that automatically records every single transaction on a public ledger, viewable by anyone on the internet, in contrast to the private ledgers used by traditional banks. This new system creates a particular need for privacy protections to avoid sharing all of one's financial dealings with all other network participants. *Second*, before OFAC intervened, Tornado Cash served as the go-to tool for law-abiding users of Ethereum to fill this critical need.

A. Financial Privacy Is Essential In The Digital Asset Sphere.

A blockchain functions like a bank's ledger: it records and tracks all transfers of data. *See, e.g.*, Appellants' Br. 9–10. But unlike a bank's

---

[7] Miller Whitehouse-Levine & Lindsey Kelleher, *Self-Hosted Wallets and the Future of Free Societies: A Guide for Policymakers*, Blockchain Ass'n (Nov. 2020), https://bit.ly/3XQDqut.

ledger—which is private, modifiable, and subject to the bank's control—blockchains like Ethereum are public, permanent, permissionless, and maintained through a decentralized network of independent computers. When a transaction occurs, this network validates it and then adds it to the "chain," where every transaction that has ever occurred in the history of that blockchain is publicly viewable and cannot ever be changed or removed. *See id.* at 10.

One consequence of this technology is that every user's interactions on the blockchain network—including any financial transactions—are public to all other users. Although the "chain" does not list anyone's name, each transaction is associated with "[p]ublic keys" (as opposed to password-like "[p]rivate keys") that may be under the control of specific persons or represent an autonomous software controlled by no one (*e.g.*, a smart contract).[8] Like an email account used to send, receive, or store messages—or a physical address in the analog world—the public key is the address that people use to send, receive, or store digital assets.[9] But

---

[8] Benedict George, *A Crypto Must-Know: Public v. Private Keys*, CoinDesk (May 11, 2023), https://bit.ly/43wFfjD.

[9] *Id.*

unlike these comparators, the blockchain is fully public, so all users can see the core components of every transaction that has ever occurred—the sender's public key, the receiver's public key, and the amount, type of asset, and time transmitted. And because users use the same public key to engage in many—if not all—of their transactions, any time a user engages in a deanonymized transaction—such as an employee paid partially through digital assets[10]—the user is deanonymizing his entire past and future transaction history to his counterparty, not to mention anyone else who may know the identity behind the user's public key. Moreover, users can sometimes be involuntarily deanonymized (or "doxxed"), as complete strangers might be able to deduce their real-world identities based on their transaction patterns or other public information.[11]

To avoid broadcasting their financial histories to the world, many digital asset holders have turned to privacy-protecting tools like Tornado

---

[10] Cloey Callahan, *Here's How Some Employees Are Being Paid in Cryptocurrencies*, WorkLife (Sept. 2, 2022), https://bit.ly/4040SXg.

[11] Adam Ludwin, *How Anonymous Is Bitcoin?*, Coin Center (Jan. 22, 2015), https://bit.ly/3Slll6Y. For this reason, blockchain is sometimes referred to as not anonymous but pseudonymous.

Cash. Such tools allow users to reclaim privacy that would be available as a matter of course in other contexts, while retaining the benefits that come with using blockchain technology. It would, for example, be unthinkable if every store could view every purchase that its customers ever made based on a single payment, or if random bystanders could view the transactions on every consumer's credit-card statements. There are innumerable understandable reasons why law-abiding people would not want their friends and neighbors to know the full details of every purchase they make, every cause they financially support, and indeed *every* transaction of *any* sort they undertake. There is nothing odd or nefarious about wanting to keep basic personal details private.

In addition to protecting privacy in general, tools like Tornado Cash allow users to protect themselves from bad actors. Particularly when a user's transaction history indicates wealth, the user risks being targeted by hackers, thieves, and other wrongdoers.[12] And when the blockchain contains enough information for a user's identity to be unmasked, these

---

[12] Andrew R. Chow, *A New U.S. Crackdown Has Crypto Users Worried About Their Privacy*, TIME (Aug. 10, 2022), https://bit.ly/3kcSwNo.

attacks can spill into the physical world, where digital asset users have been the victims of crimes ranging "from simple robberies to home invasions, kidnappings, torture, and even murder."[13]

Moreover, the need for privacy is heightened for certain, particularly sensitive transactions. Digital asset users often prioritize anonymity when supporting politically charged causes, for fear of reprisal or government sanction.[14] For example, one of the plaintiffs in this case has stopped facilitating digital asset donations to support Ukrainian relief efforts, for fear that he and other like-minded donors will be targeted by Russian agents and state-sponsored hackers. Am. Compl. ¶ 49. Likewise, privacy can be paramount when users engage in deeply personal transactions, such as a patient paying for medical procedures or a survivor of sexual assault crowdfunding expenses for

---

[13] Rob Price, *Kidnapped for Crypto: Criminals See Flashy Crypto Owners as Easy Targets, and It Has Led to a Disturbing String of Violent Robberies*, Bus. Insider (Feb. 9, 2022), https://bit.ly/3xAtavI.

[14] Zachary Halaschak, *Canadian Crackdown on Truckers Highlights Privacy Benefits of Cryptocurrency*, Wash. Examiner (Feb. 24, 2022), https://bit.ly/42tU1rw.

their recovery.[15]   Without privacy, users may feel forced to forgo transactions like these. *E.g.*, *id.* ¶¶ 46–49.

B. Tornado Cash Is An Autonomous Technological Tool to Preserve Financial Privacy.

Before OFAC's sanctions, Tornado Cash enabled Americans to protect their privacy while using Ethereum. And many availed themselves of it: as the most popular privacy tool on Ethereum, Tornado Cash has attracted more than 12,000 unique users, who have executed more than $8 billion in transactions.[16] The vast majority of such privacy-protecting transactions—more than 75 percent of transacted funds, according to OFAC's analysis of Tornado Cash and similar tools—has been licit. *See* Appellants' Br. 38–39 (citing ROA.930, 1111, 1189, 1191–95).

---

[15] Brooke Becher, *U.S. Sanctions on Tornado Cash: What Does This Mean for Crypto?*, Built In (Nov. 1, 2022), https://bit.ly/3KmqDNB; Leigh Cuen, *Sexual Assault Survivor Uses Crypto to Crowdfund Anonymously*, CoinDesk (Sept. 13, 2021), https://bit.ly/3IhWmfV.

[16] *Tornado Cash Analysis*, Dune, https://bit.ly/3kjYg7T (current as of June 1, 2023); *cf. Tornado Cash Alternatives*, Elliptic (Oct. 11, 2022), https://bit.ly/3U2FuzD (comparing Tornado Cash with its much-smaller competitors).

Tornado Cash is composed of strings of open-source code that independent developers have published to Ethereum. *See* Am. Compl. ¶¶ 1, 9–10. It operates autonomously via "smart contracts" that are programmed to self-execute certain actions when prompted by Ethereum users. *See* Appellants' Br. 11. Each smart contract is assigned a public address, similar to a user's public key, with which any user can engage. *See id.* at 10. The core Tornado Cash smart contracts are known as "pools," which are simply code protocols through which users can route digital asset deposits and withdrawals.[17] The pools are programmed to automatically generate, upon a deposit, a randomized key through which the depositing user can later withdraw funds.[18] Further, the pools are non-custodial, which means that users can only withdraw the specific funds that they submit and retain full control of their funds between deposit and withdrawal.[19] In other words, thanks to the unique power of blockchain technology, no person other than the user to whom the assets

---

[17] Alex Wade et al., *How Does Tornado Cash Work?*, Coin Center (Aug. 25, 2022), https://bit.ly/3Z0Qnnf.

[18] *Id.*

[19] *Id.*

belong has control over those assets.   Tornado Cash thus supplies a

secure mechanism for users to protect their anonymity by severing the

public connection linking all their Ethereum deposits and withdrawals.

Another key feature of the Tornado Cash pools is that they have

been programmed to be autonomous and immutable. This means nobody

owns them, controls them, or can alter or terminate them. Although the

pools originally were programmed to allow a designated "operator" to

update their coding, a 2020 update revoked this functionality for all

active pools.[20]

These features distinguish the Tornado Cash *software*—which is

non-custodial and fully autonomous—from privacy *services* owned or

operated by persons or entities.[21]   These latter services (unlike

autonomous software) facilitate privacy by taking control of users' funds

---

[20] *Id.*

[21] For an example of an owned-and-operated privacy service, see
the Blender.io currency mixer, which OFAC separately sanctioned
earlier in 2022. *U.S. Treasury Issues First-Ever Sanctions on a Virtual
Currency Mixer, Targets DPRK Cyber Threats*, U.S. Dep't of the Treasury
(May 6, 2022), https://bit.ly/3FHi9xd.

to shuffle them with other users' funds.[22]　And in contrast to Tornado

Cash, such users *do not* maintain custody of their funds.[23]

The only non-autonomous features of Tornado Cash are entirely

distinct from the core privacy-protecting software.[24]　For instance, the

DAO—or decentralized autonomous organization—relied upon by OFAC

conducts "non-essential activities to support continued development"

related to Tornado Cash.[25]　The DAO consists of anyone who holds

"TORN" governance tokens—in other words, anyone who wants to be

involved, for whatever duration they choose.[26]　It facilitates the creation

of secondary Tornado Cash-related features, such as a "Relayer Registry"

that helps Tornado Cash users find "relayers"—*i.e.*, persons acting as

conduits who can help process users' withdrawals from the Tornado Cash

---

[22]　Wade et al., *supra* note 17.

[23]　*Id.*

[24]　*See generally id.* (explaining the various Tornado Cash-related addresses).

[25]　Peter Van Valkenburgh, *Tornado Cash Is No "Golem." It's a Tool for Privacy and Free Speech*, Coin Center (Oct. 26, 2022), https://bit.ly/3KrYQLL; *see also* David Shuttleworth, *What Is a DAO and How Do They Work?*, Consensys (Oct. 7, 2021), https://bit.ly/3yYbpHB.

[26]　Wade et al., *supra* note 17.

pools, so as to maximize users' privacy.[27]   But the registry offers an entirely *optional* function; Tornado Cash users can make full use of the pools through non-registered relayers or without any relayers at all. *See* Appellants' Br. 14–15. And contra OFAC, the DAO and its non-essential services are entirely distinct from the pools themselves.   That core Tornado Cash software exists and functions regardless of the DAO.

II.   THE TORNADO CASH SANCTIONS ARE UNLAWFUL.

OFAC's sanctions have upended the lawful use and utility of Tornado Cash for its many users. With no forewarning, OFAC invoked its authority under Executive Orders 13,722 and 13,694, as amended, to sanction Tornado Cash. 87 Fed. Reg. 68,578, 68,579–80 (Nov. 15, 2022). Those Orders empower OFAC to sanction "persons" who have provided support to, respectively, the North Korean government and certain malicious cyber activities. 80 Fed. Reg. 18,077 (Apr. 2, 2015), *amended by* 82 Fed. Reg. 1 (Jan. 3, 2017); 81 Fed. Reg. 14,943 (Mar. 18, 2016). OFAC claimed it could lawfully target the Tornado Cash software protocol because the software had been used by money launderers

---

[27] *Id.*

affiliated with the North Korean government.[28]   OFAC thus added the

Tornado Cash smart contracts (*i.e.*, software code) to a list of "individuals,

groups, and entities" whose "assets are blocked and [whom] U.S. persons

are generally prohibited from dealing with."[29]   This is the first time

OFAC has ever attempted to sanction free-standing computer software,

rather than focus on the bad actors that misuse it.[30]

OFAC's sanctions forbid Americans from interacting with the

various Ethereum addresses that make up the Tornado Cash software,

87 Fed. Reg. at 68,578–79, under threat of six-figure civil fines and, for

willful violations, up to 20 years' imprisonment, 50 U.S.C. § 1705(b)–(c).

The sanctions have stranded countless Americans who were holding

funds in the Tornado Cash pools: these law-abiding citizens are no longer

permitted to access their assets unless they obtain a discretionary special

---

[28]   *Treasury Designates DPRK Weapons Representatives*, U.S. Dep't of the Treasury (Nov. 8, 2022), https://bit.ly/3ElWEkS.

[29]   *Specially Designated Nationals and Blocked Persons List (SDN) Human Readable Lists*, U.S. Dep't of the Treasury, https://bit.ly/3Z4MJYR (last updated Nov. 17, 2023).

[30] Alex Thorn et al., *OFAC Sanctions Tornado Cash: Issues & Implications*, Galaxy (Aug. 10, 2022), https://bit.ly/3IhYe8r.

15

license from OFAC,[31] which is available only on a "case-by-case basis" with no estimate as to "how long this review might take."[32]   And Americans may violate the sanctions through no fault of their own: because blockchain technology allows peer-to-peer transfers from one wallet directly to another without requiring the recipient to consent to the transfer, Ethereum users can become liable—subject only to OFAC's prosecutorial discretion—whenever someone transfers them digital assets via Tornado Cash.[33]   In that situation, the person is trapped through no fault of their own—they have no ability to reject the funds and would commit an additional sanctions violation if they remitted the funds.

OFAC's sanctions are unlawful. Because OFAC lacks statutory authority to sanction software like Tornado Cash, it has acted "in excess

---

[31] *Frequently Asked Questions #1079*, U.S. Dep't of the Treasury, https://bit.ly/3KdJpFd (last updated Nov. 8, 2022).

[32] *Frequently Asked Questions #58*, U.S. Dep't of the Treasury (Sept. 10, 2002), https://bit.ly/3MjYtnp.

[33] *Frequently Asked Questions #1078*, U.S. Dep't of the Treasury, https://bit.ly/3nMvjD2 (last updated Nov. 8, 2022); *see, e.g.*, Mat Di Salvo, *Tornado Cash User 'Dusts' Hundreds of Public Wallets—Including Celebs Jimmy Fallon, Steve Aoki and Logan Paul*, Decrypt (Aug. 9, 2022), https://bit.ly/3Ij9m5d.

of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(C). This Court should reverse the decision below.

A. OFAC's Sanctions Exceed Its Statutory Authority.

OFAC's sanctioning authority is circumscribed by Executive Orders 13,722 and 13,694 and the statutes those orders invoke. The orders authorize OFAC to designate "persons" for sanctioning pursuant to three statutes. The International Emergency Economic Powers Act, which both orders invoke, empowers the Executive to deal with national emergencies by blocking "transactions involving[] any property in which any foreign country or a national thereof has any interest." 50 U.S.C. § 1702(a)(1). The North Korea-focused order invokes two further statutes, the United Nations Participation Act and the North Korea Sanctions and Policy Enhancement Act, as supplemental authority for blocking "person[s]" and "property." 22 U.S.C. §§ 287c(a), 9214. But the autonomous Tornado Cash software is not "property"—much less the "property" of the nonexistent Tornado Cash "person." There is thus no statutory basis for OFAC's sanctions.

1. The Autonomous Tornado Cash Software Is Not "Property."

To be property, an item must be a thing that is owned. Courts[34] and dictionaries[35] have both recognized this capacity as a defining characteristic of property.   And OFAC's regulatory definition of "property" embraces the term's ordinary meaning: the regulations simply provide a list of illustrative examples, all of which are items typically understood as belonging to individuals or entities, followed by a catch-all for "any other property."   31 C.F.R. §§ 510.323, 578.314.   Under the canons of *noscitur a sociis* and *ejusdem generis*—which respectively establish that "a word is known by the company it keeps" and that a general catch-all following specific enumerated examples should be "'construed to embrace only objects similar in nature to those objects enumerated by the preceding specific words'"—this commonality means that the Tornado Cash software can fall into OFAC's definition of

---

[34] *E.g.*, *United States v. Blagojevich*, 794 F.3d 729, 736 (7th Cir. 2015); *Haze El Bey Express Tr. v. Hill*, No. 20-cv-3516, 2021 WL 3829162, at *3 (S.D. Tex. Apr. 22, 2021).

[35] *E.g.*, *Property*, Oxford English Dictionary (2d ed. 1989); *Property*, Webster's New World Dictionary of the American Language (college ed. 1968); *Property*, Webster's Third New International Dictionary (1961).

18

"property" only if the software shares this critical feature. *See Yates v. United States*, 574 U.S. 528, 545 (2015) (plurality op.).

Here, the autonomous Tornado Cash software is not and cannot be owned by anyone, much less by the Tornado Cash "person" conjured by OFAC. With the 2020 update making the code for the pools permanent and unalterable, no one can exercise any "dominion" or other essential indicia of ownership over them.[36] No one person or group has the right to possess the software, ability to transfer ownership to any other person or group, or ability to otherwise alter the software to satisfy the sanctions' stated purpose of "bring[ing] about a positive change in behavior."[37] The Tornado Cash software protocol is simply a feature affixed to the Ethereum ecosystem, much as any other immutable feature—like sun or wind in nature—can be harnessed but not owned. The Tornado Cash software thus exists entirely independent of any person or group, and so OFAC cannot sanction it as anyone's "property."

---

[36] *See Property*, Black's Law Dictionary (5th ed. 1979) (defining "property" as including the rights to possess, use, exclude, and transfer).

[37] *Treasury Designates DPRK Weapons Representatives*, *supra* note 28.

To maneuver around this reality, the District Court incorrectly suggested that the Tornado Cash smart contracts could be considered "unilateral contracts," therefore falling within the OFAC definition's inclusion of "contracts of any nature whatsoever." *Van Loon v. Dep't of Treasury*, __ F. Supp. 3d __ , 2023 WL 5313091, at *9 (W.D. Tex. Aug. 17, 2023). This conclusion ignores the *noscitur a sociis* canon. Under that rule, courts should interpret every category in a list of terms to be of similar breadth, even when the list includes a seemingly broad descriptor such as "'any.'" *Yates*, 574 U.S. at 543. Thus, just as the other examples in the OFAC definition clearly encompass only items subject to ownership—such as "money," "merchandise," and the like—"contracts" should likewise be subject to this prerequisite. 31 C.F.R. §§ 510.323, 578.314.

Indeed, the cases cited by the District Court only underscore that ownership is a threshold issue. As the District Court recognized, smart contracts can be "contracts" in the sense that they are agreements between a "buyer and seller being directly written into lines of code." *Van Loon*, 2023 WL 5313091, at *9 (quoting *Rensel v. Centra Tech, Inc.*, No. 17024500-CIV, 2018 WL 4410110, at *10 (S.D. Fla. June 14, 2018)).

Thus, for the Tornado Cash software to be a "contract," there must be a counterparty acting in the role of seller. But no one associated with Tornado Cash, which was designed from the start as open-source software code, ever acted as a seller offering a contract. *See* Appellants' Br. 10–11. And even if anyone had at an earlier point, they permanently abandoned that role with the 2020 update's conversion of Tornado Cash to be fully autonomous. *Cf. Cerajeski v. Zoeller*, 735 F.3d 577, 581 (7th Cir. 2013) ("'Abandonment' in property law … means that the owner gives up all claims to the property, thus pitching it back into the public domain, where it is available for reappropriation.").

2. There Is No Tornado Cash "Person."

Nor is Tornado Cash a "person" under any reasonable understanding of the term. OFAC's regulations define a legal person as "an individual or entity." 31 C.F.R. §§ 510.322, 578.313. Tornado Cash—software—is neither.

OFAC's assertion that it has sanctioned a Tornado Cash "entity" that purportedly owns the autonomous software likewise does not withstand scrutiny—not only because nobody "owns" that software as detailed above, but also because there is no Tornado Cash "entity"

regardless. An entity is "a partnership, association, trust, joint venture, corporation, group, subgroup, or other organization." *Id.* §§ 510.305, 578.305. Each of these examples shares a common characteristic: it is a body with a "separate and distinct existence," an "organization … that has an identity separate from those of its members."[38] But the "entity" that OFAC proffers is a supposed "Tornado Cash organization" composed of the software developers who originally coded the smart contracts (but retain no control over the software), and the Tornado Cash DAO (which, as explained above, has no ability to affect the code in any way).[39] This is not a group with the requisite "separate and distinct existence" to constitute an entity that would be a cognizable person.

Outside of OFAC's own lumping, there is no indication that these discrete actors share any sort of "organizational structure."[40] For example, there is no contemporaneous evidence proving the existence of

---

[38] *Entity*, Merriam-Webster.com, https://bit.ly/3XLLxst (last visited Nov. 19, 2023).

[39] *Frequently Asked Questions #1095*, U.S. Dep't of the Treasury (Nov. 8, 2022), https://bit.ly/3zSNV7n. OFAC defines the developers to include both the Tornado Cash "founders" and others who have aided in the development of Tornado Cash. *Id.*

[40] *Id.*

such an organization; pointing to any kind of ongoing, intentional relationship between the developers and DAO; or suggesting that the public perceived them as intertwined. An organization cannot exist merely on OFAC's say-so. Thus, even if identifying an entity associated with Tornado Cash sufficed under the statute—which it does not—OFAC has not done even that.

Tellingly, there is no Tornado Cash "person" even under the test set out by the District Court. According to the District Court, the developers and DAO are together an "association" if they are (1) "a body of individuals" that (2) "furthers a common purpose." *Van Loon*, 2023 WL 5313091, at *8. But at most, the developers and DAO are two sets of individuals with similar interests; the District Court identified no evidence that they have and are "*combined* to execute" a common purpose in partnership. *Id.* at *7 (emphasis added) (cleaned up). Nor could they with respect to Tornado Cash: neither the developers nor the DAO have any control over the sanctioned Tornado Cash smart contracts, which exist entirely independent of both.

B. Any Statutory Doubt Must Be Resolved Against OFAC.

OFAC exceeded its statutory authority for the reasons discussed above, but the Plaintiffs need not prove that much to prevail. Under fundamental principles of statutory interpretation—whether the major-questions doctrine, the constitutional-avoidance canon, or the rule of lenity—the Court should resolve any ambiguity against OFAC. Courts regularly apply such doctrines in cases with national security implications, and it should do the same here. *See, e.g.*, *Boumediene v. Bush*, 553 U.S. 723, 787–92 (2008).

1. The Major-Questions Doctrine Requires That OFAC's Authority Must Be Construed Narrowly.

The major-questions doctrine establishes that OFAC's powers here should be construed narrowly. That doctrine requires an agency to identify a clear congressional statement before it can "bring about an enormous and transformative expansion in [its] regulatory authority." *Util. Air Regul. Grp. v. EPA*, 573 U.S. 302, 324 (2014). This case would effect such an expansion because OFAC's sanctions depend on re-interpreting the core terms in OFAC's authorizing statutes—"persons" and "property"—to go far beyond any traditional or recognizable definition of those terms to give OFAC near-boundless authority.

24

Although this arrogation most immediately affects digital assets—alone a trillion-dollar industry—OFAC's claim of sweeping authority is equally applicable to any or all other industries. Absent clear congressional authorization, this power-grab must fail.

2. The Constitutional-Avoidance Canon Also Requires That OFAC's Authority Be Construed Narrowly.

OFAC's powers likewise should be construed narrowly as a matter of constitutional avoidance. Courts must interpret ambiguous statutory language in a way that avoids "serious doubt[s]" about a statute's constitutionality if it is "fairly possible" to do so. *Nielsen v. Preap*, 139 S. Ct. 954, 971 (2019) (quotation marks omitted). And the Tornado Cash sanctions raise at least two serious constitutional conflicts.

First, the sanctions cannot withstand First Amendment scrutiny. Because they indiscriminately target both bad actors and law-abiding Tornado Cash users, the sanctions "burden substantially more" speech and association "than is necessary to further the government's … interests." *Ward v. Rock Against Racism*, 491 U.S. 781, 799 (1989); *cf. Green v. Miss USA, LLC*, 52 F.4th 773, 800 n.25 (9th Cir. 2022). Here, the government could have directly sanctioned the North Korea groups that misuse Tornado Cash, just as it has sanctioned malign digital asset

users on other occasions.[41]   Instead, it has attempted to categorically

sanction a software those groups misuse.   In the process—and

apparently, intentionally[42]—OFAC has cut ordinary Americans off from

a means of engaging in anonymous financial speech and associations.

That overbroad choice unconstitutionally chills First Amendment rights,

notwithstanding the alternative methods of speech and association that

may exist: "[t]he risk of a chilling effect … is enough, because First

Amendment freedoms need breathing space to survive."   *Ams. for*

Prosperity Found. v. Bonta, 141 S. Ct. 2373, 2389 (2021) (cleaned up).

Second, OFAC's sanctions cannot be squared with the Due Process

Clause of the Fifth Amendment, which bars the deprivation of property

without due process of law. The amount of process required depends on

a balancing of interests, but the government generally must provide

individuals "notice and an opportunity to be heard before depriving them

---

[41] Thorn et al., *supra* note 30.

[42] *See* Scott Chipolina & James Politi, *US Treasury Imposes Sanctions on 'Crypto Mixer' Over Alleged Laundering*, Fin. Times (Aug. 8, 2022), https://bit.ly/3XJqGG7 (quoting a "senior Treasury official" as saying that the sanctions were to "'send a really critical message'" against services like Tornado Cash and "'designed to inhibit Tornado Cash or any sort of reconstituted versions of it'").

of their property." *Zevallos v. Obama*, 793 F.3d 106, 116 (D.C. Cir. 2015).

Here, OFAC provided *zero* pre-deprivation notice before sanctioning

Tornado Cash and instead blocked all American Tornado Cash users

from accessing their funds.[43]

There was no cause for that denial of notice. Although courts often

uphold sanctions imposed without pre-deprivation notice based on a fear

of asset flight, *see Al Haramain Islamic Found., Inc. v. U.S. Dep't of

Treasury*, 686 F.3d 965, 985 (9th Cir. 2012), that rationale has no force

here. Because the Tornado Cash pools are immutable and the Tornado

Cash software does not maintain custody or control over the assets held

in the pools, these assets cannot be frozen the way money in a bank can

be. And because the pools remain available for all to use, the targeted

North Korean wrongdoers *are not actually blocked from retrieving their

assets.*[44] Only law-abiding American users are thwarted by their respect

for the law.

---

[43] *Frequently Asked Questions #1079*, *supra* note 31.

[44] *See* Tim Hakki, *BitKeep Hacker Moves $1M in Binance Coin Through Tornado Cash*, Decrypt (Oct. 18, 2022), https://bit.ly/3xIALIF; *Tornado Cash Mixer Sanctioned After Laundering Over $1.5 Billion*, Elliptic (Aug. 8, 2022), https://bit.ly/3FTdNDa.

3. The Rule of Lenity Further Confirms That a Narrower Interpretation Is Necessary.

To the extent there is any remaining doubt, the rule of lenity further underscores that any ambiguity must be resolved against OFAC. This rule ensures that "legislatures and not courts … define criminal activity," *United States v. Bass*, 404 U.S. 336, 348 (1971), by requiring that ambiguous provisions be construed in favor of criminal defendants, *Lockhart v. United States*, 577 U.S. 347, 361 (2016). The rule applies to any "statute with criminal sanctions," even in cases that arise in a "noncriminal context," *Kasten v. Saint-Gobain Performance Plastics Corp.*, 563 U.S. 1, 16 (2011), because any statute must be "interpret[ed] … consistently" across cases, *Leocal v. Ashcroft*, 543 U.S. 1, 11 n.8 (2004). Accordingly, because OFAC's authorizing statutes criminally proscribe the "willful[]" violation of sanctions, *see* 22 U.S.C. §§ 287c(b), 9214(f); 50 U.S.C. § 1705(c), any ambiguity about the scope of what is sanctionable must be narrowly construed.

CONCLUSION

OFAC's sanctions cannot be squared with a proper understanding of the autonomous Tornado Cash software or OFAC's governing statutes. If allowed to stand, this overreach will have sweeping consequences—

weakening the digital asset industry, jeopardizing law-abiding Americans' financial privacy, and effecting a vast expansion of OFAC's power. This Court should reverse the decision below and direct the entry of summary judgment for the Plaintiffs.

Dated: November 20, 2023   Respectfully submitted,

                                            /s/ Mark W. Rasmussen

Eric Tung   Mark R. Rasmussen
JONES DAY   JONES DAY
555 South Flower Street,   2727 North Harwood Street,
Fiftieth Floor   Suite 500
Los Angeles, CA 90071   Dallas, TX 75201
(213) 489-3939   (214) 220-3939
                                            mrasmussen@jonesday.com

                                            Alexis Zhang
                                            JONES DAY
                                            51 Louisiana Avenue, N.W.
                                            Washington, DC 20001
                                            (202) 879-3939

        Counsel for Amicus Curiae

CERTIFICATE OF COMPLIANCE

Pursuant to Fed. R. App. P. 32(g), the undersigned attorney for Appellant certifies that the foregoing brief

(i)   complies with the type-volume limitation in Fed. R. App. P. 32(a)(7)(B) and Circuit Rule 32(c) because it contains 5,295 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

(ii)   complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) and Circuit Rule 32(b) because this brief has been prepared in a proportionally spaced typeface using Microsoft Office Word 2016 in 14-point Century Schoolbook Std.

/s/ *Mark W. Rasmussen*
Mark W. Rasmussen

CERTIFICATE OF SERVICE

In accordance with Circuit Rule 25(a), I hereby certify that on November 20, 2023, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Fifth Circuit by using the CM/ECF system. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

<div align="right">

/s/ Mark W. Rasmussen
Mark W. Rasmussen

</div>