IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, Plaintiff, v. ROMAN STORM and ROMAN SEMENOV, Defendants.	Hon. Katherine Polk Failla No. 1:23-cr-00430-KPF

BRIEF FOR *AMICUS CURIAE* BLOCKCHAIN ASSOCIATION IN SUPPORT OF DEFENDANT ROMAN STORM'S MOTION TO DISMISS

Stephanie Brooker (*pro hac vice pending*)
Matt Gregory (*pro hac vice forthcoming*)
Nick Harper (*pro hac vice*)
Tessa Gellerson (*pro hac vice*)
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington D.C. 20036-5306
(202) 955-8500
Sbrooker@gibsondunn.com
Mgregory@gibsondunn.com
Nharper@gibsondunn.com
Tgellerson@gibsondunn.com

Counsel for Amicus Curiae the Blockchain Association

April 5, 2024

Corporate Disclosure Statement

Counsel for *amicus curiae* Blockchain Association certify that *amicus curiae* has no parent corporation and no publicly held corporation owns 10% or more of *amicus curiae*'s stock.

Table Of Contents

Page

Table Of Authorities

Page(s)

Cases

Statutes

Table Of Authorities

Page(s)

Regulations

Other Authorities

Interest of *Amicus Curiae*[1]

The Blockchain Association is the leading nonprofit membership organization dedicated to promoting a pro-innovation policy environment for the digital asset economy. The Association endeavors to achieve regulatory clarity and to educate policymakers, regulators, courts, and the public about how blockchain technology can create a more secure, competitive, and consumer-friendly digital marketplace. The Association represents nearly 100 member companies reflecting the wide range of the blockchain industry, including software developers, infrastructure providers, exchanges, custodians, investors, and others supporting the public blockchain ecosystem.

Introduction

The money-transmitter charges against Defendants, Tornado Cash founders Roman Storm and Roman Semenov, are premised on a fundamental misunderstanding of how the relevant technology works and what the law requires.[2] Longstanding statutes, regulations, and agency guidance make clear that a money-transmitting business exists only when the business exercises control over the assets transmitted. It is *not* enough, as recent FinCEN guidance for the digital asset industry explains, for an intermediary to merely be a part of a money-transmitting transaction. Unless the intermediary exercises total independent control over the assets, money-transmitter liability cannot attach. Indeed, FinCEN's own guidance recognizes that "suppliers of … anonymizing software" are not money transmitters. Accepting the government's theory here would upset the careful lines FinCEN has drawn to define money-transmitting businesses in the

[1] Counsel for *amicus curiae* certify that no counsel for a party authored this brief in whole or in part, and no person other than *amicus curiae* made any monetary contribution to its preparation or submission.

[2] *Amici curiae* Coin Center and DeFi Education Fund ably explain why Counts One and Three of the indictment should also be dismissed. Coin Center Br., ECF 43; DeFi Br., ECF 39.

context of digital assets, with severe consequences—including an unprecedented and unjustifiable risk of criminal liability—for the digital asset industry and the technology sector generally.

The main flaw in the government's theory is that it fails to allege that Defendants had total independent control over any assets transferred using Tornado Cash, which FinCEN has recognized is a necessary component of a money-transmitting business under the relevant statutory and regulatory provisions. The distinct tools and technologies at issue in the indictment lack that critical hallmark of a money-transmitting business, either separately or in the aggregate.[3] Most critically, although third parties can use the Tornado Cash protocol (i.e., computer software) to transmit digital assets, at no point during the relevant period charged in the indictment did Defendants exercise control over any of those digital assets. Indict. ¶ 80.

Without control over the assets, Defendants cannot be held liable as money transmitters. This Court should reject the theory underlying the indictment, which would eliminate a foundational requirement of the criminal statutes concerning money transmitters, raise serious fair-notice concerns, and have far-reaching consequences for the digital asset industry.

Background

I. The Money-Transmitting Laws

Count Two of the indictment alleges that Defendants conspired to operate an "unlicensed money transmitting business" in violation of 18 U.S.C. § 1960(b). As relevant here, Section 1960 defines an unlicensed money-transmitting business as "a money transmitting business" that either: (1) fails to register with FinCEN under the Bank Secrecy Act or to comply with related regulations or (2) involves the transmission of funds that the defendant knows to be derived from a criminal

[3] What the indictment refers to as the "Tornado Cash service" is a series of separate open-source, self-executing software tools and technologies that run on the Ethereum blockchain. *See* Indictment ("Indict.") ¶¶ 1–3, 9–10. For ease of reference, the Association refers to these distinct technologies as "Tornado Cash."

offense or used to promote or support unlawful activity. *Id.* § 1960(b)(1)(B), (C). The statute defines "money transmitting" as "transferring funds on behalf of the public." *Id.* § 1960(b)(2).

Section 1960's definition of a "money transmitting business" is materially identical to the Bank Secrecy Act's definition of that same phrase. *See* 31 U.S.C. § 5330(d)(1) (any business that engages in the "transmission of … funds" or facilitates "the transfer of money"). Courts therefore have looked to the Bank Secrecy Act and its implementing regulations to interpret the scope of Section 1960. *See, e.g.*, *United States v. Harmon*, 474 F. Supp. 3d 76, 101 (D.D.C. 2020) ("virtually no substantive difference"); *United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 92 n.10 (D.D.C. 2008) (same); *United States v. Budovsky*, 2015 WL 5602853, at *8 (S.D.N.Y. Sept. 23, 2015) ("an indictment need only allege a violation of [the Bank Secrecy Act's] implementing regulations to sufficiently allege a violation of" Section 1960(b)(1)(B)).

Regulations promulgated under the Bank Secrecy Act by FinCEN require "[m]oney transmitter[s]" to register with FinCEN, and define a "[m]oney transmitter" to be either: (1) a "person that provides money transmission services," or (2) any "other person engaged in the transfer of funds." 31 C.F.R. § 1010.100(ff)(5)(i). "[M]oney transmission services" means the "acceptance . . . *and* . . . transmission" of funds "to another location or person by any means." *Id.* (emphasis in original). Among other carveouts, FinCEN regulations exempt from the definition of "money transmitter" individuals who merely provide "the delivery, communication, or network access services used by a money transmitter to support money transmission services." *Id.* § 1010.100(ff)(5)(ii)(A). FinCEN guidance has also long recognized that a person must exercise "total independent control" over the digital assets being transmitted to be a money transmitter.[4]

[4] *E.g.*, FinCEN, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* ("2019 FinCEN Guidance") (§ 4.2) (May 9, 2019), tinyurl.com/3fsns8ts.

II. Overview of Tornado Cash

Tornado Cash is part of the now more than two-trillion-dollar digital asset economy.[5] The digital asset industry is built upon blockchains, which may be accessed by anyone and are not controlled by an administrator. A blockchain is a distributed ledger: a database maintained by many computers that can record and verify data across the entire network.[6] Among the many benefits of blockchain technology are that it is more efficient, transparent, and inclusive than legacy financial technology.[7] But because of the public nature of the blockchain, most transactions are not private by default, unlike legacy financial transactions. Instead, they are "recorded on a public ledger," meaning "the movement of funds … can be traced." Indict. ¶ 7.

The transparency of the public ledger can generate serious privacy concerns for digital asset owners. By default, the public can view and track users' transactions on the blockchain. And although blockchain transactions typically do not reveal personally identifying information (e.g., names or social security numbers), the transactions often can be traced to particular individuals through the use of blockchain analytics and other techniques. If a blockchain user is deanonymized, anyone can see the core components of every transaction the user has ever executed in the past—including the amount, asset type, and time of transmission. This is akin to publishing an individual's entire credit card transaction history online.[8] Understandably, digital asset users generally do not want their personal transaction history to be made public. For example, an employee who is paid in digital assets may not want her employer (or others) to be able to track

[5] Brady Dale, *Bitcoin's Market Cap Breaks $1T, Taking Overall Crypto Market to $2T*, Axios (Feb. 14, 2024), bit.ly/3U1Nv9q.

[6] *See generally What Is Cryptocurrency?*, Coinbase, bit.ly/3lSamp7.

[7] *Id.*

[8] *See* Adam Ludwin, *How Anonymous Is Bitcoin?*, Coin Ctr. (Jan. 22, 2015), bit.ly/3Slll6Y; *see also* Bitcoin.org, *Protect Your Privacy*, bit.ly/4ahOvf7.

every digital asset transaction she has ever made or will ever make.[9] Individuals who donate to politically charged causes and organizations also may not want to broadcast their actions.[10] The public nature of the blockchain can also expose individuals with significant wealth in digital assets to attacks by blackmailers, kidnappers, and other wrongdoers.[11]

Tornado Cash solves these problems by protecting the privacy of individuals conducting digital asset transactions, the vast majority of which are legitimate.[12] It does so by pooling the transactions of many different digital asset users. Until recently, Tornado Cash was the most popular privacy-protecting tool on Ethereum, the second-largest blockchain.[13]

To evaluate the government's money-transmitter allegations, it is necessary to understand four technical concepts underlying Tornado Cash: "smart contracts," "relayers," "secret notes," and the "user interface."

Smart contracts. Smart contracts are immutable, autonomous software programs that can be programmed to perform specific tasks on blockchains. They are used to power blockchain

[9] Cloey Callahan, *Here's How Some Employees Are Being Paid in Cryptocurrencies*, WorkLife (Sept. 2, 2022), bit.ly/3VGGf45.

[10] Andrew R. Chow, *A New U.S. Crackdown Has Crypto Users Worried About Their Privacy*, Time (Aug. 10, 2022), bit.ly/3TLOjOj (founder of Ethereum used Tornado Cash to donate to Ukrainian causes); Lia Holland, *Statement: Treasury's Clumsy Approach to Tornado.cash Is a threat to the Future of Financial Privacy*, Fight for the Future (Aug. 9, 2022), bit.ly/3VMVDMd (similar regarding contributions to Planned Parenthood).

[11] Rob Price, *Kidnapped for Crypto: Criminals See Flashy Crypto Owners as Easy Targets, and It Has Led to a Disturbing String of Violent Robberies*, Business Insider (Feb. 9, 2022), bit.ly/3J5dRAX.

[12] *E.g.*, Pls.' Mot. for Summ. J. at 23, *Van Loon v. Dep't of Treasury*, No. 1:23-cv-312-RP (W.D. Tex. Apr. 5, 2023), ECF 41 (compiling government concessions in the certified agency record, including that more than 75% of funds sent to anonymizing protocols, like Tornado Cash, are licit, and money laundering accounted for only "0.05%" of digital asset transaction volume in 2021); *Crypto Money Laundering: Four Exchange Deposit Addresses Received Over $1 Billion in Illicit Funds in 2022*, Chainalysis (Jan. 26, 2023), tinyurl.com/4vfbm5rw (estimating that only between 10–25% of digital assets sent to anonymizing protocols in 2022 were from illicit sources).

[13] *Tornado Cash Analysis*, Dune, bit.ly/3kjYg7T; *Tornado Cash Alternatives*, Elliptic (Oct. 11, 2022), bit.ly/3U2FuzD.

applications, such as applications for exchanging and lending digital assets. Once a smart contract is deployed (i.e., published) to a blockchain, it operates autonomously (i.e., without human intervention). Anyone in the world can deposit digital assets into a smart contract, which can automatically carry out a particular task in response. By default, smart contracts are also immutable once deployed. This means that unless they are initially programmed to allow for updatable functionality, they cannot be altered, removed, or controlled by anyone—even the people who created them.

Underpinning Tornado Cash is a collection of smart contracts on the Ethereum blockchain. Key to its operation are its "pool" smart contracts, which allow a user to deposit digital assets into a pool containing other users' digital assets, and then withdraw those assets from the pool at a later time to a digital wallet of the user's choosing.[14] All Tornado Cash smart contracts are encoded to be non-custodial, meaning that users maintain total ownership and control over their assets at all times.[15] A user always withdraws the very same assets she deposited. This is different from other anonymizing services that take control of deposited digital assets, mix them together, and then reshuffle them among different users in withdrawals.[16] Rather than taking custody of users' digital assets and mixing them together, Tornado Cash provides anonymity by requiring deposits to be made in particular denominations (e.g., 0.1, 1, 10, or 100 units); different pools also exist for each denomination, so the identity of any given depositor cannot easily be traced to a corresponding withdrawal based on the amount of the deposit.[17]

---

[14] *Understanding Tornado Cash, Its Sanctions Implications, and Key Compliance Questions*, Chainalysis (Aug. 30, 2022), bit.ly/49ljLZu.

[15] *How Does Tornado Cash Work?*, Coin Center (Aug. 25, 2022), bit.ly/3VGzDCI.

[16] *Id.*

[17] *Id.*; *see also* Indict. ¶ 19.

The government's indictment acknowledges that since at least May 2020, the Tornado Cash pool smart contracts have been immutable, meaning that Defendants have had no ability to modify, remove, or control them.[18] A handful of other smart contracts associated with Tornado Cash were, however, programmed to allow for updates.[19] But none of those smart contracts gave Defendants any control over user assets.

Relayers. Relayers are third parties who provide an additional layer of anonymity for Tornado Cash users. Indict. ¶ 24. Use of relayers is entirely optional. *Id.* ¶¶ 24, 25. Relayers solve the following problem: To withdraw digital assets from the Tornado Cash smart contracts, a user must pay a "gas" fee in the form of Ether, a digital asset native to the Ethereum blockchain. The user can pay the gas fee using the digital wallet receiving the withdrawal. But then the user would have to pre-load that wallet with Ether, which would be publicly viewable on the blockchain and potentially make the wallet traceable to the user. *Id.* Relayers provide a privacy-protecting alternative. They process withdrawal requests on behalf of users, including paying the gas fee. *Id.* In return, relayers recoup the gas fee plus a service fee. The indictment suggests relayers "deduct" these fees from the withdrawn amount, *id.* ¶ 24, but that is not the case. The user sets the fees when she generates the proof, and relayers and users receive funds directly and separately from the pool smart contract—the relayer recoups the fees, and the user receives the remainder of the withdrawal amount.[20] Starting around March 2022, a smart contract called the "Relayer Registry"

[18] Indict. ¶ 26.

[19] *How Does Tornado Cash Work?*, Coin Center, *supra*.

[20] Benjamin Gruenstein et al., *Working Paper 1: Secret Notes and Anonymous Coins: Examining FinCEN's 2019 Guidance on Money Transmitters in the Context of the Tornado Cash Indictment* at 16 & n.24, Int'l Acad. of Fin. Crime Litigators (Sept. 2023), tinyurl.com/2t8ctfyj.

began compiling a list of relayers meeting certain criteria that users could elect to process their withdrawals.[21] Indict. ¶ 30.

Secret note. In order to use Tornado Cash, a person must create a "secret note." A secret note is a random number that users either can select on their own or have generated for them.[22] It functions like a password, allowing the user to make deposits to and withdrawals from Tornado Cash pools. Unlike a traditional online password that may be known both to a user and the website, however, for Tornado Cash the user is at all times the "*only* person with access to the secret note." Indict. ¶ 15 (emphasis added). A user selects the secret note on her personal device, and never reveals it to anyone else when making deposits or withdrawals.[23] Tornado Cash accomplishes this through the use of advanced cryptographic algorithms.

To make a deposit into Tornado Cash, a person runs her secret note through a cryptographic "hashing" algorithm on her personal device. Indict. ¶ 15. The algorithm takes input data (here, the secret note) and generates a unique digital fingerprint of the input data, known as a "hashed value."[24] The hashed value is distinct from the secret note, and there is no way to use the hashed value to reverse engineer the secret note.[25] The user then shares the hashed value—but not the secret note—with the Tornado Cash smart contract, along with her deposit.[26]

The user does not reveal her secret note when she makes a withdrawal either. Instead, the user provides a "zero knowledge proof" to the Tornado Cash smart contract. This algorithm, which again runs on the user's personal device, generates a mathematical "proof" that the user actually

[21] *How Does Tornado Cash Work?*, Coin Center, *supra*.
[22] Technically, the secret note is two numbers. But for simplicity, we refer to it as a single number. Gruenstein et al., *Working Paper*, *supra*, at 12 & n.21.
[23] *Id.* at 12.
[24] *How Does Tornado Cash Work?*, Zellic (Apr. 6, 2023).
[25] Gruenstein et al., *Working Paper*, *supra*, at 12.
[26] *Id.*

has the secret note.[27] Much like the hashed value, the proof "reveals nothing about the secret note."[28] It is this proof—not the secret note—that the user shares with the smart contract (or a relayer) in order to validate the withdrawal.[29]

In short, the *only* inputs the smart contract and relayers receive related to the secret note are the hashed value and the proof. At all times, the user retains exclusive control over the secret note, which is necessary to make deposits and withdrawals on Tornado Cash. In other words, nobody can transfer the user's assets without the user's participation.

The indictment contains two unexplained allegations that could suggest that the secret note *is* shared with the smart contract and relayers: that users "enter the secret note" on the user interface, which sends the secret note "to a smart contract," and that relayers "transmit the secret note to the … smart contract." Indict. ¶¶ 16, 18, 24. These allegations, taken literally, are inaccurate for the reasons just explained—they fail to grasp how hashing algorithms and zero knowledge proofs function. They are also inconsistent with the government's acknowledgement elsewhere in the indictment that "the customer would be the only person with access to the secret note." *Id.* ¶ 15.

User interface. A "user interface" is a user-friendly website or application that allows users to interact with a smart contract on their web browsers or smart phones.[30] Anyone can design a user interface for a particular smart contract, not just the creators of the smart contract. And users can choose to forgo user interfaces altogether and instead interact with the smart contract directly. Indict. ¶ 13. Generally, however, a user interface is not on the blockchain and therefore does not itself interact with any of the user's digital assets. The user interface simply facilitates

[27] Gruenstein et al., Working Paper, *supra*, at 13.
[28] *Id.*
[29] *Id.*
[30] *Id.* at 10 (citing Indict. ¶ 13); Frederick Munawa, *Decentralized Mixer Tornado Cash Makes Its User Interface Open-Source*, CoinDesk (July 7, 2022), bit.ly/3U3eGk0.

the user's interaction with the smart contract. The Tornado Cash user interface does so in two ways. The user interface can assist a user with generating the secret note and with running the algorithms necessary to obtain the hashed values and proofs using the secret note. The user interface also helps generate the transaction message that allows a user to communicate her requested action—for example, how much to deposit or withdraw—to the smart contract. *See id.* ¶ 15; Coin Center Amicus Br. at 5–6, 7–8. But, through all of this, the secret note never leaves the user's local browser and is not shared with Defendants or any other party.

Argument

I. To be a money-transmitting business, Tornado Cash must have had control over the digital assets at issue.

A. Section 1960 requires control.

Section 1960 requires a money transmitter to have control over the value being transmitted, meaning the independent ability to effect the movement of the assets at issue. Section 1960 liability hinges on the "transfer[]" or "transmission" of funds. 18 U.S.C. § 1960(b)(1)(C), (b)(2). The Bank Secrecy Act also defines "money transmitting business," in part, based on the "transmission" of funds. 31 U.S.C. § 5330(d)(1). Both words—"transfer" and "transmission"—presuppose control over the underlying value being transmitted. "[T]ransfer" means "[t]he act of transferring," "conveyance or removal from one place, person, etc. to another," "to convey from one person, place, or situation to another."[31] Similarly, "transmit," the verb form of "transmission," means "to send or convey from one person or place to another."[32] One cannot transfer or transmit something (e.g., cash, a package) without control over the thing being transferred.

[31] *Transfer*, Merriam-Webster, bit.ly/3J2OXC5; *Transfer*, Oxford English Dictionary, bit.ly/3TXGoyJ.

[32] *Transmit*, Merriam-Webster, tinyurl.com/mw9f22mn.

The Second Circuit understands what it means to be a money transmitting business the same way, explaining in one case that such a business "*receives* money from a customer and then, for a fee paid by the customer, *transmits* that money to a recipient." *United States v. Velastegui*, 199 F.3d 590, 592 (2d Cir. 1999) (emphases added). Similarly, the Second Circuit explained that a violation of Section 1960 occurs when an individual "maintained possession" of and then "transfer[red]" someone else's funds. *United States v. Bah*, 574 F.3d 106, 114 n.6 (2d Cir. 2009).

Control is implicit in an individual's receipt of something that the individual then transfers to someone else—for example, a delivery driver takes food from a restaurant, has complete control over it, and then transfers it to a consumer's house. In contrast, a person who gives her hungry friend a ride to the restaurant and back is providing transportation, not transferring food from the restaurant to her friend. The Third Circuit recognized this common-sense understanding of the word "transfer" in the context of a statute criminalizing the transfer of drugs, endorsing an interpretation that "centers on possession and control." *United States v. Semler*, 858 F. App'x 533, 536 (3d Cir. 2021) (discussing the meaning of "transfer" in the context of the Controlled Substances Act). Transferring money (or digital assets) is no different.

Other courts have agreed, holding that liability cannot accrue under Section 1960 or analogous state statutes when a defendant lacked control over the underlying value. *See, e.g.*, *United States v. $1,370,851.62 in U.S. Currency*, 2010 WL 11650916, at *6 (S.D. Fla. Oct. 6, 2010) (no Section 1960 liability because defendant "did not *first* receive money from its clients"); *Givelify, LLC v. Dep't of Banking & Sec.*, 210 A.3d 393, 401–02 (Pa. Commw. Ct. 2019) (petitioner did not "transmit[] money" under a state analog of § 1960 because he did not "obtain" the money nor was the money "deposited into an account directly owned or controlled by [him]").

B. FinCEN regulations require control.

FinCEN has also consistently taken the view that control over the underlying value is a necessary prerequisite to money-transmitter liability. FinCEN's regulations define a "[m]oney transmitter" as "[a] person that provides money transmission services," and further define "money transmission services" as the "acceptance . . . *and* . . . transmission" of currency or the "transfer of funds." 31 C.F.R. § 1010.100(ff)(5)(i)(A), (B). As with "transmit" and "transfer," control over the underlying value is inherent in the meaning of "acceptance." To "accept" something means "to receive (something offered) willingly" or to "take or receive (something offered)."[33] Courts have interpreted "receive" in other criminal statutes to mean "to accept an object and to have the ability to control it." *United States v. Dobbs*, 629 F.3d 1199, 1203–04 (10th Cir. 2011); *United States v. Stanley*, 896 F.2d 450, 451 (10th Cir. 1990) (interpreting "receive" to mean "to acquire control, in the sense of physical dominion or apparent legal power to dispose of the [item]"). Control is also present in traditional forms of money transmission (e.g., physical receipt of a check that a money transmitter exchanges for cash). *See, e.g.*, *United States v. Han*, 637 F. Supp. 3d 527, 545 (N.D. Ill. 2022) (defendant "picked up … cash," then used his discretion to purchase and sell goods to hide the funds' source, before "transferr[ing] th[e] cash to … China"); *United States v. Neumann*, 2022 WL 3445820, at *7 (S.D.N.Y. Aug. 17, 2022) (defendant "accept[ed]," and thereby obtained control of "cash," and then wrote a check "payable to an entity").

FinCEN's regulations also expressly exempt from the definition of "money transmitter" individuals who merely provide "the delivery, communication, or network access services used by a money transmitter to support money transmission services." 31 C.F.R. § 1010.100(ff)(5)(ii). This exception, referred to as the "software exemption," confirms that it is not enough for someone

[33] *Accept*, Merriam-Webster, bit.ly/3J248LJ; *Accept*, Oxford English Dictionary, bit.ly/3PNTPPd.

to provide a service that is a necessary link in the chain of the money transmission. Instead, to be a money transmitter, a person must (at least) have control over the funds being transmitted.

C. FinCEN guidance also requires control.

FinCEN guidance further confirms the centrality of control to the money-transmitter inquiry—and does so in the context of digital assets. The guidance makes clear that "control" exists *only* when an entity or individual has the ability to independently direct the movement of the underlying assets. In its 2019 guidance document ("2019 Guidance" or "guidance"), FinCEN emphasizes, for example, that the regulatory treatment of individuals who act as "intermediaries between the owner of the value and the value itself is not technology-dependent" and, instead, turns on several factors, including "whether the person acting as intermediary has *total independent control* over the value." 2019 FinCEN Guidance at 15 (§ 4.2) (emphasis added). In other words, an entity is not a "money transmitter" unless it has the independent ability to transfer the assets on the user's behalf—it is insufficient for the intermediary to merely be a necessary part of the transaction. Without control over the assets, money-transmitter liability cannot attach. *Id.*

FinCEN's guidance provides examples of how this works in practice. Most relevant here, the guidance explains that an "anonymizing software provider is not a money transmitter."[34] That is because "suppliers of tools (communications, hardware, or software) that may be utilized in money transmission, like anonymizing software, are engaged in trade and not money transmission."[35] By contrast, anonymizing service providers—those who "*accept*[] value from a customer and transmit[] the same or another type of value to the recipient"—are money transmitters because they control the value at issue.[36]

[34] 2019 FinCEN Guidance § 4.5.1(b) (May 9, 2019).
[35] *Id.*
[36] *Id.* § 4.5.1(a) (emphasis added).

Another example relates to "multiple-signature wallet providers," which are "entities that facilitate the creation of wallets" for digital assets that "for enhanced security, require more than one private key [i.e., password] for the wallet owner(s) to effect transactions." 2019 FinCEN Guidance at 17 (§ 4.2.2). These entities are not "money transmitter[s]" even if they "house[]" a "second key" that is used to "validate[] and execute[] the transaction," because, even though they are necessary to the transaction, the "value belongs to the owner" and the intermediary "does not have total independent control over the value." *Id.*

The guidance also explains that digital asset trading platforms and decentralized exchanges are not money transmitters if they provide only a forum where buyers and sellers of digital assets post their offers and bids, and the parties themselves settle any matched transactions off-platform. 2019 FinCEN Guidance at 23–24 (§ 5.1). If, however, a platform purchases the digital assets from the seller—thereby indisputably taking control of the assets—and then sells the assets to the buyer, it is a digital asset exchanger and falls within the definition of money transmitter. *Id.* The guidance also says that digital asset sellers during initial coin offerings (the initial sales of digital assets) are money transmitters because they are authorized to issue and redeem the new units of the digital asset—and they have discretion over the exercise of that authority. *Id.* at 25 & n.76 (§ 5.2).

Each of these examples, taken from FinCEN's own guidance, makes clear that independent control over the underlying asset being transferred is an essential part of the money-transmitting offense—it is not enough for a protocol to merely play some role in the transmission of assets, or to provide a platform that allows for the transmission of assets. In other words, even if a platform is *necessary* for a transmission to occur, its developers are not money transmitters unless they have sufficient control such that they can transfer the assets all by themselves.

II. The government has not adequately alleged that Defendants exercised control over the digital assets on Tornado Cash.

Count Two of the indictment—alleging that Defendants operated an unlicensed money-transmitting business—fails to allege that Defendants exercised total independent control over the digital assets on Tornado Cash. A user's secret note is the *only* way to effect transmissions of digital assets into and out of the Tornado Cash pools, and therefore possession of the secret note is the single determining factor for control. And the indictment concedes that none of the Defendants ever had access to the secret note. Indict. ¶ 15. That is sufficient to dispose of Count Two completely.[37]

Nor could the government cure its defective indictment. The government cannot pursue a money-transmitter theory based on the deposit or withdrawal of users' digital assets into a pool smart contract, for two independent reasons. First, as explained above, *supra* at 5–7, the pool smart contracts operate autonomously and do not control digital assets. Instead, they are non-custodial, meaning that the user, and not the smart contract, maintains total ownership and control over the user's assets at all times.[38] Second, the government concedes that Defendants relinquished any control they had over the pool smart contracts by May 2020—before the operative timeframe for Count Two. Indict. ¶ 26. Thus, the government cannot establish that Defendants "knowingly conduct[ed], control[ed], manage[d], supervise[d], direct[ed], or own[ed] all or part of" the smart contracts during the relevant period. 18 U.S.C. § 1960(a).

The government also cannot premise money-transmitter liability on Defendants' alleged control over Tornado Cash's user interface. Indict. ¶¶ 14, 26, 30. The indictment suggests users

[37] Defendant Storm raises an additional alternative and independent ground for dismissing Count Two, but this brief focuses exclusively on the absence of any relevant allegations of control. ECF 30 at 24–25.

[38] *See How Does Tornado Cash Work?*, Coin Center, *supra*.

executed transactions by "enter[ing] the secret note" through the user interface. *Id.* ¶¶ 16, 18. But selecting a secret note through the user interface does not share that secret note with any other party, including Defendants, because this function is performed locally on the user's device.[39] The user creates the secret note and runs the hashing and proofing algorithms all on her personal device. The user interface merely allows users to interact with the Tornado Cash smart contracts and relayers, including by creating the secret note and by communicating information—but, critically, never the secret note—to the smart contracts and relayers. The user interface therefore does not give Defendants control over users' digital assets.

The same holds true for allegations related to relayers. The indictment alleges that Defendants maintained a smart contract containing a registry of relayers and that "relayer[s] transmit[ted] the secret note to the Tornado Cash smart contract." Indict. ¶¶ 16, 18, 24, 27–31, 68. But the indictment does not allege that Defendants controlled any specific relayers—only that they "maintained" the relayer registry. *Id.* ¶ 68. Thus, even if Defendants helped develop the algorithm that decided which relayers appeared on the relayer registry, Defendants had no control over relayers' actions. Moreover, relayers themselves never exercised total independent control over users' digital assets because they never received users' secret notes. *Id.* ¶ 15 (the user is the "only person with access to the secret note"). The relayers are merely a tool that a person can use to access the value connected to the secret note. Thus, money-transmitter liability could not attach even if the indictment had alleged that Defendants controlled the relayers.

For similar reasons, Defendants fall within the regulatory "software exemption" for the provision of "network access services," 31 C.F.R. § 1010.100(ff)(5)(ii)(A), which provides an independent basis for dismissing Count Two. FinCEN has conceded that a developer or seller of

[39] Gruenstein et al., *Working Paper*, *supra*, at 11–12; *see also* supra at 8.

software is exempt from Bank Secrecy Act obligations as a money transmitter so long as it does not also use the software to "engage as a business in accepting and transmitting currency." 2019 FinCEN Guidance at 3 (§ 1.1). This holds true even if the "purpose of the software is to facilitate the sale of virtual currency."[40] This exemption protects software developers whose innovation (much like any tool) might be misused for nefarious purposes. And the exemption applies with full force here. Defendants merely created the anonymizing protocols that allow users to transmit (and thereby attempt to anonymize) their digital asset transactions through Tornado Cash pools. That their software is used by others to facilitate the transmission of digital assets does not mean that Defendants are engaged in the business of accepting and transmitting digital assets themselves.

III. Elimination of the control requirement threatens serious adverse consequences for the blockchain economy.

The government's theory of money-transmitter liability is an abrupt about-face from past precedent and its adoption would cause serious adverse consequences for the digital asset industry. For years, industry members have relied on FinCEN's regulations and 2019 Guidance in developing and investing in their services. And the regulations require total independent control and independently carve out an exception for entities that merely provide "the delivery, communication, or network access services used by a money transmitter to support money transmission services." 31 C.F.R. § 1010.100(ff)(5)(ii)(A).

FinCEN cannot change its mind about the scope of this exception or adopt a novel interpretation of what it means to be a money transmitter without effecting that change through notice and comment. *See, e.g.*, *Am. Fed'n of Gov. Emps., AFL-CIO v. FLRA*, 777 F.2d 751, 759 (D.C. Cir. 1985) (an agency "seeking to repeal or modify a legislative rule promulgated by means

[40] FinCEN, FIN-2014-R002, *Application of FinCEN's Regulations to Virtual Currency Software Development and Certain Investment Activity* at 2 (Jan. 30, 2014), bit.ly/3vsaOzX.

of notice and comment rulemaking is obligated to undertake similar procedures to accomplish such modification or repeal"). And FinCEN has done no such thing; to the contrary, its regulations remain in force to this day. So does its 2019 Guidance, which plainly requires that an entity have total independent control over the underlying assets. The Department of Justice's effort to impose *criminal* liability for conduct in compliance with FinCEN's longstanding regulations and guidance also deprives not only Defendants but the entire digital asset industry of fair notice of what the law requires.

Extending Section 1960's reach to the facts of this case also would have an immediate and lasting chilling effect on the creation and use of anonymizing protocols for digital assets and rob digital asset owners of a legitimate method of protecting their privacy. There is nothing inherently suspicious about a desire for privacy in digital asset transactions, just as there is nothing suspicious about privacy in traditional financial transactions. Privacy is implicit in the traditional financial system—nobody wants their bank to post their account history online—and digital asset owners should not be denied the same privacy for blockchain transactions.

Yet if the government's expansive interpretation of Section 1960 were adopted, developers of anonymizing protocols would risk criminal liability under the Bank Secrecy Act despite not being in control of funds. *See* 18 U.S.C. § 1960(b)(1)(B), (C). Worse, compliance with the Bank Secrecy Act could be impossible for developers, meaning the government's interpretation is tantamount to a ban on anonymizing protocols. Compliance could be impossible for a range of reasons. For example, once protocols are deployed, there may be no centralized management who can attempt to comply with reporting or other requirements. Further, once a protocol is deployed, it becomes immutable; it is impossible for a developer to decommission the software even if it is being misused for criminal purposes. Extension of the money-transmitter laws to developers of

anonymizing protocols would therefore put this industry out of business at the expense of the public's legitimate desire for privacy.

And there is no valid justification for the government's overreach. To the extent the government is concerned with digital assets being used to launder money or fund terrorism, it can effectively prevent those problems through enforcement of other laws and by targeting illicit actors directly, for example, by sanctioning digital asset wallets associated with illicit actors. It should not pile on by contorting the money-transmitting laws to fit the same underlying conduct.

Adoption of the government's theory could also have other unintended consequences. It may chill the development of other protocols such as peer-to-peer protocols, which allow for the transfer of digital assets between individuals and entities, or protocols that allow users to deposit funds into a smart contract, for fear that these protocols may also fall within the government's overbroad definition of a money transmitter. And it could call into question the "software" exemption entirely, which provides a legitimate carve out for individuals engaged in *trade*—i.e., in the sale of software, not in money transmission.[41] It could also portend the risk of criminal liability for other digital asset technologies, such as decentralized exchanges, that FinCEN has long recognized are not money transmitters if they provide only a forum for buyers and sellers of digital assets to post bids and offers that are then settled off-platform.[42] Erosion of the control requirement would make it difficult to distinguish these exchanges from anonymizing protocols or other entities the government is attempting to regulate as money transmitters. And the government's theory also could have unanticipated ramifications outside the digital asset context, because FinCEN's guidance provides that "[t]he regulatory interpretation of the [Bank Secrecy

[41] 2019 FinCEN Guidance at 20 (§ 4.5.1(b)).

[42] *Id.* at 24 (§ 5.1); U.S. Dep't of Treasury, *Illicit Finance Risk Assessment of Decentralized Finance* at 7 (Apr. 2023) (noting that DeFi services may be money transmitters, however, if they "accept[] and transmit[] virtual assets from one person to another person or location").

Act] obligations of persons that act as intermediaries between the owner of the value and the value itself is not technology-dependent." 2019 FinCEN Guidance at 15 (§ 4.2). Accordingly, other technologies could also potentially be treated as money transmitters under the government's new interpretation of Section 1960. This would undermine national security objectives overall because innovation in this space would be driven offshore where it will be much more difficult for U.S. regulators to monitor bad actors and for law enforcement to hold them accountable.

Eliminating the control requirement would also destabilize the Bank Secrecy Act's regulatory scheme. Many of the Act's regulations presume that covered entities have control over the underlying assets. For example, the suspicious activity reporting requirements, which require money transmitters to report suspicious transactions of more than $2,000, are triggered when assets go "by, at, or through" a covered entity, and the currency transaction reporting requirement, which requires money transmitters to report currency transactions over $10,000 conducted by, or on behalf of, one person, as well as multiple currency transactions that aggregate to be over $10,000 in a day, are triggered when assets go "by, through, or to" a covered entity. 31 C.F.R. § 1022.320(a)(2) (suspicious activity reports for money services businesses); *id.* § 1010.311 (currency transaction reporting requirement). Elimination of the control requirement would raise thorny questions about whether a money transmitter who does not have control over transmitted assets must comply with these and other regulations.

Conclusion

The Court should dismiss Count Two of the indictment. At minimum, the Court should make clear that Section 1960 requires that a money transmitter have total independent control of the assets at issue and should reject the government's apparent theory to the contrary.

Dated: April 5, 2024

Respectfully submitted,

/s/ *Stephanie Brooker*
Stephanie Brooker (*pro hac vice pending)*
Counsel of Record
Matt Gregory (*pro hac vice forthcoming)*
Nick Harper (*pro hac vice)*
Tessa Gellerson (*pro hac vice)*
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
(202) 955-8500
Sbrooker@gibsondunn.com
Mgregory@gibsondunn.com
Nharper@gibsondunn.com
Tgellerson@gibsondunn.com

Counsel for Amicus Curiae the Blockchain Association