UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

THE UNITED STATES OF AMERICA, v. ROMAN STORM, ET AL., Defendants.	Case No. 23 Cr. 430 (KPF)

DEFENDANT ROMAN STORM'S REPLY TO THE GOVERNMENT'S OPPOSITION TO RULE 29 MOTION

Brian E. Klein
Keri Curtis Axel
Becky S. James
Kevin M. Casey
Viviana Andazola Marquez
Waymaker LLP
515 S. Flower Street, Suite 3500
Los Angeles, California 90071
(424) 652-7800

David E. Patton
Christopher Morel
Hecker Fink LLP
350 Fifth Ave, 63rd Floor
New York, New York 10118
(212) 763-0883

Attorneys for Roman Storm

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

CASES

STATUTES

OTHER AUTHORITIES

I. PRELIMINARY STATEMENT

This Court should grant Roman Storm's motion and acquit on all three counts.

As a threshold matter, the government has failed to prove venue for any count. Accurate communications with an attorney who happened to be in the District did not further any charged conspiracy. There is no proof that any payment by Mr. Storm was received in Manhattan, much less that any such receipt would have been foreseeable to him. A hacker's use of the Tornado Cash website *prior to* his hacking activity did not further the charged conspiracies. There is insufficient evidence that any relevant Dragonfly chat occurred when a representative was in Manhattan, or furthered a charged conspiracy, or that Mr. Storm reasonably could have foreseen that the representative was in this District. These reeds are simply too thin to support venue.

Turning to the merits of the case, Mr. Storm should be acquitted of all three counts. As this Court made clear at the pretrial conference: "This isn't a negligence case. It's a willfulness case." (7/8/2025 Tr. at 58:2-3.) But time and again, the government has insisted that Mr. Storm is guilty, not because of willful criminal conduct, but because he should have done more to prevent criminals from using the Tornado Cash software he helped develop and made available to the public. The government is therefore attempting to do exactly what troubled this Court—convict Mr. Storm "for not doing what he was not legally required to do." (7/8/2025 Tr. 59:4-6.)

As to the specific charges, the conviction on Count Two was improper because Tornado Cash was not a money transmitter, as, by design, it did not control any user's proceeds. This Court should revisit its prior ruling on control having now seen the uncontroverted trial evidence, but, even if it does not, it should nevertheless grant this motion because there is no evidence that Mr. Storm *believed* Tornado Cash to be an unlicensed money transmission business and *agreed* to operate it as such, much less willfully. The overwhelming evidence shows that he instead desired to build a permissionless, noncustodial protocol that permitted users to conduct their own

transactions without the control or involvement of an intermediary money transmitter. This was a lawful goal accomplished lawfully.

Counts One and Three fail because they are also based on the government's improper negligence theory. This is evident from the government's expert witness testimony, its closing arguments, and its opposition brief, all of which contend that Mr. Storm had a legal duty either to: (1) stop the bad actors who were allegedly using Tornado Cash to launder funds or (2) shut down or modify the Tornado Cash website and UI. But the government does not say where that duty comes from. It cannot be the Bank Secrecy Act, since the government does not contend that Tornado Cash or its developers were regulated under the Act. What the government means is that it believes Mr. Storm had a duty to implement AML and KYC-like safeguards in the Tornado Cash protocol, implicitly relying on a negligence-based theory that cannot support criminal liability.

Counts One and Three fail for additional reasons, among them: The government cannot meet the standard for willfulness—the highest intent standard under the law—based on its negligence theory. The only "affirmative conduct" by Mr. Storm that the government cites is consistent with the conduct of developing and maintaining the lawful Tornado Cash software, not with the conduct to advance criminal conspiracies. Nor can the government meet the criminal conspiracy standard because it has not shown, and cannot show, that any alleged co-conspirator of Mr. Storm committed (or ever agreed to commit) the acts of money laundering and sanctions evasion that could make him vicariously liable. The government ignores the overwhelming legal authority Mr. Storm has marshalled on this point, which requires Mr. Storm's acquittal.

Further, as to Count One, the government has no evidence that Mr. Storm agreed to conduct specific transactions with the requisite knowledge that they (1) contained proceeds of

criminal activity and (2) were designed to conceal such proceeds. The government disputes this knowledge element, but it is well supported by Supreme Court and Second Circuit precedent. And as to Count Three, conspiracy to violate sanctions, the government has no evidence that Mr. Storm provided a "service" "to" or "for the benefit of" the Lazarus Group. Moreover, the charge violates the informational materials exemption in the IEEPA.

Finally, while the government dismisses Mr. Storm's constitutional arguments out of hand, its opposition only further proves that Mr. Storm's constitutional rights are at stake here: the government has stretched each of the statutes beyond recognition and is seeking to use this criminal prosecution to impose legal duties that have no basis in statute or regulation. The prosecution of Mr. Storm has gone too far: strict scrutiny and the rule of lenity apply.

Construing the evidence in the light most favorable to the government, there is insufficient evidence to convict Mr. Storm on any count; he should be acquitted.

****

As a resource for this Court, Mr. Storm has distilled the undisputed facts concerning the technology at issue cited throughout the parties' Rule 29 briefing in the Technology Facts Appendix ("TFA"), which is below. It is organized by topic; topics are referred to in the brief by relevant number; and the facts in it are incorporated by reference where cited.

II. THE GOVERNMENT DID NOT ESTABLISH VENUE IN THIS DISTRICT, REQUIRING DISMISSAL OF ALL COUNTS

Whenever it is faced with challenges to its asserted bases for venue, the government develops new, previously unasserted bases. But the new grounds in its opposition fare no better than the ones presented in the pretrial conference (7/11/2025 Tr. at 18-20 (Tom Schmidt messages; Bloomberg reporter communications; protocol available on a "website" to "customers" available and used in New York)), or at the Rule 29 argument and summations (Tr.

1633-40, 2380-82 (BitMart communications; payments to Infura; "payments for maintenance of and operation" of website available and used in New York; Tom Schmidt messages)). Despite promises that its evidence would be sufficient to prove venue, the government failed to provide any basis that does not rely on impermissible speculation to find an overt act committed in the Southern District of New York in furtherance of the conspiracy that was reasonably foreseeable to Mr. Storm. The government has failed to establish this important requirement, which in criminal cases is "not merely [a] matter of formal legal procedure, but [a] matter of constitutional right." *United States v. Conteh*, 2 F. App'x 202, 203 (2d Cir. 2001) (cleaned up).

The government's opposition overstates the factual record and relies on speculation as a substitute for reasonable inferences. *See United States v. Quattrone*, 441 F.3d 153, 169 (2d Cir. 2006) (a court "may not credit inferences within the realm of possibility when those inferences are unreasonable"); *see also United States v. Purcell*, 967 F.3d 159, 189 (2d Cir. 2020) (finding no venue in the Southern District of New York because "the government's theory of venue is entirely speculative"). A reasonable inference "is not a suspicion or a guess[; it] is a reasoned, logical decision to conclude that a disputed fact exists on the basis of another fact that is known to exist." *United States v. Pauling*, 924 F.3d 649, 656 (2d Cir. 2019) (internal quotations omitted).

A. Communications with BitMart's Attorney

The critical question underlying whether the founders' communications with BitMart's attorney, Joseph Evans, provides a basis for venue on Count One, as the government claims (*see* Opp. at 20), is whether they "used the [communications] to further the objectives of the conspiracy." *United States v. Rommy*, 506 F.3d 108, 122 (2d Cir. 2007). They did not.[1]

[1] This Court questioned this theory of venue during the Rule 29 conference. (Tr. 1634-35 ("Please, sir, are you suggesting that part of the conspiracy to commit money laundering was

First, the founders' communications with Mr. Evans were not false. The government claims that the following statement, made *in response to a request for tracing assets, user information, and freezing transactions*, is a lie:

> Our company does not have any ability to affect any change or take any action with respect to the Tornado Cash protocol – it is a decentralized software protocol that no one entity or actor can control. For that reason, we are unable to assist with respect to any issues relating to the Tornado Cash protocol.

(GX 1011; Opp. at 20.) Every part of that statement was undeniably true.

The government argues it was a lie because of changes that were made to the UI and hypothetical ways Tornado Cash could have been built in a different manner than it was. (*See* Opp. 21 (citing Tr. 1064 (discussing changes to the UI); *id*. at 23 n.2 (citing Tr. 1160 (Werlau testifying about user registry).) But any such systemic changes were irrelevant to Mr. Evans's inquiry because they would not have enabled the founders to trace and return any funds to BitMart. In fact, neither Mr. Werlau nor any other witness identified anything the founders could have done at the time of Mr. Evans's outreach to provide him the requested information. The government's claim that "Mr. Werlau's testimony established that the defendant could have provided victims with precisely the type of information Mr. Evans was requesting," referring to transactional information, is meritless. (Opp. at 23 n.2 (citing GX 1005 and Tr. 1160).) Mr. Werlau's cited testimony was clearly about the type of information the founders could *hypothetically* collect and provide "under the system I propose," (Tr. 1160:16-21), not the information that the founders actually had in their possession.

Similarly, the communications between the founders from February 14, 2022, months after Mr. Evans's outreach, do not support the government's argument. (*See id*. at 22 (citing GXs

---

blowing off inquiries from victims and law enforcement . . . ?" and "So had he not answered, no; but having answered . . . in your estimation falsely, that's an overt act, and an act that gets you venue[?]").)

2059-2-T, 2060-T).) First, GX 2059-2-T is a voice note where Roman Semenov explains the theoretical possibility of the DAO creating a "special multisig where the [authorities]" could request information about stolen funds, but noting that while this is theoretically possible "the community doesn't . . . like this at all" because of the community's interest in decentralization. Second, Mr. Storm's message in GX 2060-T is in the context whether Tornado Cash should charge a protocol fee and merely acknowledges that, despite a project's aim for decentralization, all DeFi projects have some centralized points. The communications did not establish that the founders had the ability to trace assets, provide user information, or freeze transactions that had already occurred, as Mr. Evans was requesting, especially at the time of his outreach. (*See id.*)

Similarly, nothing in the record supports an inference that the founders sought to dissuade Mr. Evans from pursuing remedies, as the government urges. (*See id*. at 23-24.) It simply does not follow that telling Mr. Evans (truthfully) that they could not assist him would keep him from going to law enforcement. *See, e.g., Pauling*, 924 F.3d at 656 (inferences must be reasonable).

Moreover, the text messages showing that the founders expressed concern about law enforcement attention are not connected in any way to the response sent to Mr. Evans, as the government claims. (*See* Opp. at 24-25.) Indeed, the cited communications all are from months later, in response to increased regulatory and criminal enforcement activity in the cryptocurrency sector and commentary from internet trolls calling them criminals—not in response to Mr. Evans's outreach. (*See id*. (citing GXs 2059-2-T (voice note from February 2022), 2043-T (chats from March 2022), 2062-T (April 2022 chats).) None of these chats is probative of the founders' intent in December 2021 to supposedly dissuade victims from seeking remedies.

B. Payments to Infura

The government advances the Infura evidence only for Counts One and Two. (Opp. at 25.) But even for those counts, the Infura payments fail to establish venue for four reasons:

(1) the lack of evidence that any payments went to a Manhattan bank account; (2) even if they did, the location of a third-party's bank account is an insufficient basis to support venue; (3) any deposits into a Manhattan-based bank account were not acts "reasonably foreseeable" to Mr. Storm; and (4) the payments do not satisfy the substantial contacts test.

1. There Is No Evidence that Any Payment Was Received in Manhattan

The record lacks any evidence to show that Peppersec directed any payment to a Manhattan bank account. Because Peppersec began paying Infura in cryptocurrency in March 2022 (*see* Opp. at 25), the only possible time period when a payment could have been directed to a Manhattan bank account was ***before*** March 2022, when Peppersec paid its invoices by credit card. (Mot. at 20). But the only invoice bearing routing information for a Manhattan-based beneficiary account (GX 851) was from March 2022. Prior to that, the government offers neither invoices nor payment records (such as the credit card processing records) to prove any Manhattan connection. Instead, the government offers only the that "a reasonable jury" could "draw the inference that the Infura bank account listed on the March 2022 invoices was the same bank account accepting payments in prior months." (Opp. at 26.) This involves at least two layers of "impermissible speculation," *Pauling*, 924 F.3d at 646: (1) speculation that Infura held a Manhattan bank account before March 2022: and (2) speculation that such a bank account is where credit card payment fees were received. Indeed, this is not merely speculation but a "sizable inferential leap[,]" *United States v. Glenn*, 312 F.3d 58, 67 (2d Cir. 2002), that this court should not countenance. The government failed to connect the Infura credit card payments to Manhattan; thus, the payments cannot support venue for Counts One or Two.

The evidence fails as to Count Two for an additional reason: the last credit card payment was on February 1, 2022. (*See* GX 849.) But the alleged Count Two conspiracy did not commence until the announcement of the "relayer algorithm[,]" which did not happen until later

in February 2022. (*See e.g.*, Indictment, Dkt. 1 at ¶ 29.) The government cites to GX 2210, a communication from Mr. Storm in November 2021 discussing an early iteration of the relayer registry idea, to stretch the Count Two conspiracy to an earlier date than it charged in the Indictment (Dkt. 1 at ¶ 80 (alleging conspiracy commenced March 2022) and the Superseding Indictment (Dkt. 109 at ¶ 7 (alleging conspiracy commenced February 2022). As such, this Court should not consider the Infura payments as a basis for venue on Count Two.

2. Even If Deposits to Infura Had Gone to a Manhattan Bank Account, That Is an Insufficient Basis on Which to Base Venue

The government assumes without authority that the mere presence of a third party's payment bank account is sufficient to confer venue. (*See* Opp. at 25.) It is not. *See United States v. Bezmalinovic*, 962 F. Supp. 435, 438 (S.D.N.Y. 1997) (finding bank's ministerial acts of debiting and crediting accounts insufficient to support venue and granting motion to dismiss).

The government argues that the use of Infura's service furthered the charged conspiracies, but it never explains how Mr. Storm's credit card payments to Infura (setting aside the lack of evidence they were ever deposited into the Manhattan-based bank account) furthered the alleged conspiracies. (*See* Opp. at 25.) The mere location of Infura's bank account, which Mr. Storm did not pay directly, made absolutely no difference to the success or failure of Tornado Cash, much less any supposed criminal conspiracy. The government's expansive venue theory is convenient because, as they point out, the Southern District of New York is home to a great many financial institutions. (Opp. at 27 n.4.) So this tenuous connection would allow almost any case to be brought in this District. *See, e.g.*, *United States v. Geibel*, 369 F.3d 682, 697 (2d Cir. 2004) (noting that defendant's conduct was "too anterior and remote to confer venue in the SDNY" and warning that to "hold otherwise would be to in effect grant the Southern District of New York carte blanche on venue") (internal quotations omitted). Just because a

third-party vendor happens to have a bank account in Manhattan does not mean that its use, utterly tangential to the alleged conspiracy, confers venue.

3. Infura's Supposed Deposits into a Manhattan-Based Bank Account Were Not Reasonably Foreseeable to Mr. Storm

Any Infura deposits into a Manhattan bank account were also not reasonably foreseeable to Mr. Storm. *See United States v. Kirk Tang Yuk*, 885 F.3d 57, 69 (2d Cir. 2018). The government's only foreseeability argument—advanced *for the first time* in its opposition—is that Peppersec's bank statements identify the pre-March 2022 Infura payments as going to a "NY" recipient with a 347-based area code. (Opp. at 26-27.) But none of the Infura exhibits tie that phone number to an address within this District. Indeed, the 347-area code services the "Bronx, Brooklyn, Queens, Staten Island, and the Marble Hill sections of the New York City metropolitan area."[2] Without more, an oblique reference to "NY" cannot support foreseeability. *See United States v. Lange,* 834 F.3d 58, 67 & n.5 (2d Cir. 2016) (declining to find venue in EDNY based on call lists containing phone numbers with the 718 area code because (1) the area code covered areas both within and outside of EDNY; and (2) the 718 phone numbers did not have corresponding addresses in EDNY); *cf. id.* at 73 (finding foreseeability to EDNY where call lists included phone numbers that did have corresponding addresses within EDNY). The government's reliance on *Kirk Tang Yuk,* 885 F.3d at 73 n.4, for the proposition that any reference to "New York" can be inferred to be a reference to the SDNY is misplaced. (*See* Opp. at 27 n.4.) The cited footnote refers to other cases (including *Lange*) where the government had *not* tried to base venue on mere references to "New York."

[2] *See* New York State Department of Public Service, *PSC Approves New Area Code for New York City Area*, https://tinyurl.com/kfuyb86p. Brooklyn, Queens, and Staten Island are in the Eastern District of New York. https://tinyurl.com/ypyvy84y.

Moreover, the "reasonably foreseeable" requirement is applied out of a recognition that the venue requirement demands "some sense of venue having been freely chosen by the defendant." *Kirk Tang Yuk*, 885 F.3d at 69. Because Mr. Storm had no control over where Peppersec's payments went, it cannot be said that he "freely chose[]" this District.

4. The Infura Payments Do Not Satisfy the Substantial Contacts Test

The government has no answer to the substantial contacts test other than to distort the caselaw. The test is not foreclosed by *Kirk Tang Yuk* (Opp. at 27), which confirmed that the substantial contacts test "offers guidance on how to determine whether the location of venue is constitutional, *especially* in those cases where the defendant's acts did not take place within the district selected as the venue for trial." *Kirk Tang Yuk*, 885 F.3d at 70 (quoting *United States v. Saavedra*, 223 F.3d 85, 93 (2d Cir. 2000)) (emphasis added). Likewise, *United States v. Rowe*, 414 F.3d 271, 279 (2d Cir. 2005), which the government cites in support, did not address the substantial contacts test other than to note that the district court found venue proper in light of the test. (Opp. at 28.)

The government never addresses the four factors, all of which favor Mr. Storm. (*See* Mot. at 22 (applying the test from *United States v. Royer*, 549 F.3d 886 (2d Cir. 2008).) The government only responds that Mr. Storm was no more prejudiced than other defendants hailed into this district (Opp. at 28), which is not the standard. Contrary to the government's claims, Mr. Storm has been prejudiced: it is exponentially more expensive, and far less convenient, for Mr. Storm to have had the case tried in Manhattan than in his district in Washington State. In any event, the test has four factors, not one, and the factors tip sharply in his favor.

C. Hacker's Use of Tornado Cash Website

As to the operation of the Tornado Cash website and its supposed use by Shakeeb Ahmed, the government cites no authority for the proposition that operating a website available

to users and accessed in this District is sufficient to confer venue. Instead, the authorities cited in support of this novel theory of venue, *Rowe*, 414 F.3d 271, *Royer*, 549 F.3d 886, and *United States v. Levis*, 488 F. App'x 481, 485 (2d Cir. 2012), are highly distinguishable. First, none of them involves the mere *operation* of a website as the act conferring venue. Second, those authorities turn on the transmission of *information* constituting the conduct of the offense on the Internet, which was in fact received by someone in the district, as the basis for venue.[3]

For instance, in *Rowe*, the Second Circuit affirmed venue where, in a chat room that was accessed in the district, the defendant engaged in the conduct constituting the offense, which was publishing a "notice or advertisement seeking or offering" child pornography. 414 F.3d at 279 (citing 18 U.S.C. § 2251(c)(1)(A)). The Second Circuit found that the defendant's Internet post offering child pornography, which could have foreseeably been accessed anywhere in the world and was in fact viewed in the district, was effectively the same as if the defendant had posted a flyer with the advertisement in the district. *Id*. Similarly, in *Royer*, the acts constituting the insider trading offense, caused by the defendants sending hundreds of messages containing misappropriated information to investors in the Eastern District of New York, who then traded in the relevant securities based on that information, was sufficient for venue. 549 F.3d at 894. Finally, in *Levis*, the acts constituting the wire fraud offense were also performed on the Internet when the defendant made the misrepresentations in a company's Form 10-K that was transmitted and relied on by an individual in the district. 488 F. App'x at 486.

[3] The government also cites *United States v. Thomas*, 74 F.3d 701, 705 (6th Cir. 1996), noting that it is cited in *Rowe* "for a similar conclusion" (Opp. at 30 & n.6), but *Thomas* involved the transmission of obscene materials where the defendants intentionally and knowingly transacted business in the district of prosecution by approving a subscriber's application to obtain the obscene materials which contained an address and phone number in the place of prosecution, and by placing a call to the subscriber who ultimately received the obscene materials in that district.

The government here does not allege that acts constituting the offense were transmitted on the Tornado Cash website and received by someone in this District. What was transmitted by the website was not illegal, and its maintenance was not an act constituting the offenses of conspiring to commit money laundering or to operate an unlicensed money transmitter. Even if they were, Mr. Ahmed's testimony would fail to provide a basis to make such an inference—he testified that he did not recall where he learned about how to increase the anonymity of his deposit and failed to identify the Tornado Cash website when asked about it. (Tr. 902.)

Moreover, contrary to the government's argument, Mr. Ahmed's use of Tornado Cash needed to "materially" further the alleged conspiracies for venue to attach. *Royer*, 549 F.3d at 896. The government claims that the defense "misreads" *Royer* as requiring materiality (Opp. at 31-32), but the government ignores *Royer*'s express limitation on venue to those acts that "materially furthered the ends of the conspiracy." *Id.* In *Royer,* what occurred in the district were acts of certain site subscribers that were "crucial to the success of the scheme." *Id.* at 895.

By contrast, Mr. Ahmed's use of Tornado Cash was not material to the conspiracies alleged in Counts One and Two. The government argues that increasing the size of the pool was material to the concealment required for a money laundering conspiracy, but it makes no argument, nor could it, that Mr. Ahmed's use had any impact. (*See* Opp. at 31.) Instead, the government argues that it was the "widely accessible" use of Tornado Cash in the "largest city in the United States" that was material. (*Id.*) But the government did not introduce evidence about the widespread use of Tornado Cash in the Southern District of New York; it only introduced evidence of Mr. Ahmed's single use. The government's argument proves too much. If the single use by Mr. Ahmed were sufficient to confer venue based on increasing the size of the pools, then *any lawful use* of Tornado Cash by anyone in the District would be sufficient to confer venue.

The government also contends that Mr. Ahmed's website use was reasonably foreseeable because the website was available world-wide. (Opp. at 32-33.) But an act that materially furthered the conspiracies is what must be foreseeable, and the mere use of the website is not such an act. *United States v. Allamon*, 2005 WL 2542905, at *3 (S.D.N.Y. Oct. 11, 2005), is likewise unavailing. Like *Rowe*, *Royer*, *and Levis*, in *Allamon*, the website transmitted the false representations at the heart of the advance fee scheme. The *Allamon* court found the allegation that the false representations were made available in the district via the website sufficient to support venue at the motion to dismiss stage.

D. Communications with Dragonfly

The communications with Tom Schmidt and Haseeb Qureshi of Dragonfly fail to confer venue on any count due to two critical deficiencies: it was not reasonably foreseeable to Mr. Storm that he was transmitting communications to this District, and the communications were not acts in furtherance of any conspiracy. (*See, e.g.*, Opp. at 33-34).

1. The Dragonfly Evidence Fails for Lack of Foreseeability

The government claims that the following facts are sufficient to establish that it was reasonably foreseeable to Mr. Storm that Mr. Schmidt was in Manhattan during their communications: (1) Mr. Schmidt was "no stranger" to Mr. Storm; (2) Mr. Schmidt was living in Manhattan when the communications took place; (3) Mr. Schmidt's phone pinged "almost exclusively" in Manhattan;[4] and (4) Mr. Schmidt had regular communications with Mr. Storm. (Opp. 39.) But none of these "facts" establishes that it was reasonably foreseeable to Mr. Storm that Mr. Schmidt was in Manhattan at the times of the communications.

[4] The government misstates the record. (*See* Opp. at 39.) As its own witness acknowledged, and his summary chart showed, Mr. Schmidt's phone pinged in places other than Manhattan about half the time. (*See* Mot. at 29 (citing GX 3001 at 7-10; and Tr. 1001).)

The sole evidence implicating New York at all—an April 1 chat (GX 2245 at 209) where Mr. Schmidt says he is "in ny"—cannot reasonably be stretched to provide foreseeability of Mr. Schmidt's whereabouts during the other chat exchanges on April 6, May 2-4, and June 9-10, much less to the March 15 messages which happened before the reference to New York. This Court previously expressed skepticism about this basis of foreseeability:

> [Y]ou speak about an ongoing relationship. Imagine that in the course of an ongoing relationship with a VC located in California, the VC sends a text to Mr. Storm saying: I am in New York, I have just seen the greatest play on Broadway, talk to you soon. And that is the entirety of the exchange. You're not going to suggest to me venue from that. Correct?

(7/11/25 Tr. at 25.) But the government is indeed suggesting venue from that. (*See* Opp. at 39.) This Court additionally asked if there were "any indication from signature blocks in the messages that this person is in New York or are they using a phone number that's 917 or 212 or something along those lines?" (7/11/25 Tr. at 26.) There was none.

Indeed, there was no evidence that Mr. Storm knew Mr. Schmidt's place of residence, or that Mr. Storm called or texted with Mr. Schmidt to a phone with a New York-based area code, or that there were any emails exchanged with a Manhattan-based address in Mr. Schmidt's signature line, or any other like-fact that would support the inference. Thus, the speculative inferences the government claims are possible, including the supposed "common-sense inference that a person can often identify information about the location of someone who they are talking to through a video-calling application like Zoom" lack any basis in fact. (Opp. at 39.)

Further, the government's opposition does not respond to a central argument raised by Mr. Storm's Motion: "NY" could refer to anywhere in New York state, or even if New York City, the Eastern District of New York. *See Lange*, 834 F.3d at 67 & n.5.

Finally, there is no evidence that Mr. Schmidt was in Manhattan during the May and June conversations. The government's only location evidence as to those conversations was American

Express records showing purchases made on the dates in question. (*See* Opp. at 38.) These records do not establish when the purchases were made or that in fact Mr. Schmidt made them.

2. The Communications Were Not in Furtherance of Any Conspiracy

The government advances no basis to construe the messages exchanged between Mr. Storm and the Dragonfly representatives as acts in furtherance of each of the conspiracies charged. "[Communications] from one district to another by themselves can establish venue in either district *as long as the calls further the conspiracy*." *Kirk Tang Yuk*, 885 F.3d at 71 (emphasis added). However, "casual conversation about past events, idle chatter between co-conspirators, or merely narrative descriptions by one coconspirator of the acts of another do not qualify as statements in furtherance of the conspiracy." *United States v. Johnson*, 469 F. Supp. 3d 193, 213 (S.D.N.Y. 2019) (collecting and quoting Second Circuit authorities about statements which are not in furtherance of a conspiracy) (cleaned up).

First, nothing in the record supports the government's interpretation of the cherry-picked March 15-18 messages, in which Mr. Schmidt raises the interest of a separate project in using "Tornado's relayer network[.]" (*See* Opp. at 34 (citing GX 2245).) The government claims that this communication was in furtherance of the conspiracies to "commit money laundering and unlicensed money transmitting" because it "promot[ed] Tornado Cash." (*Id.*) But nothing about discussing another project using Tornado Cash's technology furthers these alleged crimes.

Second, the government claims that on April 1, 2022, Mr. Storm asked Mr. Schmidt "about a communication he had received from Dragonfly's auditor," but the email in the message is not in evidence, nor do the messages identify the email as having come from "Dragonfly's auditor[.]" (*See id.* at 35 (citing GX 2245).) The messages clearly do not pertain to the operation of Tornado Cash in any way. Moreover, the subsequent discussion about the

Dragonfly representatives' whereabouts likewise amount to "idle chatter[,]" which is completely untethered from any of the supposed conspiracies.

Third, the April 6, 2022 messages (which lack any reference to Mr. Schmidt's whereabouts) include a request by Mr. Storm that Schmidt ping TORN holders to vote on a proposal. But there is no evidence that this proposal was in furtherance of a money laundering or money transmitting conspiracy. To arrive at that conclusion, one would have to make speculative inferences about the proposal's contents, which the government does not even attempt.

Fourth, the government's efforts to construe the May 2, 2022 messages, GX 1372 (again, containing no indication of location), as concerning efforts to bring "Tornado Cash to 'full compliance'" ignore the messages' plain text. (Opp. at 36.) Mr. Storm's opening message reads "we are brainstorming an idea… has to be under new brand name basically fork of tornado cash but with KYC/AML[.]" (*See* GX 1372.) The government insists that it is irrelevant whether a separate project is being discussed, but that cannot be so. (Opp. at 37.) The finder of fact would have to completely disregard that the message is gauging interest in a separate, new project rather than making changes to Tornado Cash. Such a conversation is "too anterior and remote to confer venue in the [District.]" *Geibel*, 369 F.3d at 697. Moreover, the government's claim that these messages reflect a conversation with Mr. Schmidt (Opp. at 36) is simply wrong; Mr. Schmidt is not a conversation participant. Even assuming Mr. Schmidt saw the messages, there is nothing about his passive receipt of them that furthered any alleged conspiracy.

Finally, the June 2022 messages (again, with no indication of whereabouts) require similarly speculative leaps. Contrary to the government's assertion (Opp. at 38), the absence of evidence of what was discussed during the Zoom call defeats an inference that the Zoom call was in furtherance of the conspiracies. *See, e.g.*, *United States v. Tomasetta*, 2012 WL 2064978, at *7

n.7 (S.D.N.Y. June 6, 2012) (declining to find that "attendance at investor meetings" were acts in furtherance of a fraud scheme where there was no evidence of the substance of such meetings).

Moreover, even assuming the conversation did involve continued funding for Tornado Cash, that was not a sufficient basis to establish venue for each of the alleged conspiracies. At most, such a conversation would have furthered the aim of continuing to operate Tornado Cash. But continuing to operate Tornado Cash was not a crime. The alleged conspiracies were to engage in money laundering, the unlawful operation of a money transmitting business with knowledge that it involved the transfer of illicit funds, and sanctions evasion under the IEEPA. There is simply no evidence that Mr. Storm and Mr. Schmidt discussed these allegedly *illegal* uses of Tornado Cash, much less that anything they discussed furthered such illegal use.

III. THE EVIDENCE WAS INSUFFICIENT TO SUPPORT THE JURY'S VERDICT ON COUNT TWO

This Court should enter a judgment of acquittal on Count Two. Mr. Storm maintains that Tornado Cash was not in fact a money transmitting business and that custody of funds is required, something that is indisputably absent here. Regardless, the government entirely failed to adduce any evidence, much less sufficient evidence to support a conviction, regarding key elements of Mr. Storm's mental state, including that he: (1) agreed to operate an unlicensed money transmission business; (2) did so willfully; (3) knew he was operating a money transmitting business; or (4) knew at the time of transmission that the funds were derived from criminal activity.

A. The Evidence Failed To Establish a Criminal Agreement To Engage in Unlicensed Money Transmitting

The government's opposition fails to address the primary problem with its criminal agreement theory as to Count Two: Mr. Storm's lack of intent to join with his co-founders in an agreement to operate a business that transmitted funds. Indeed, the evidence was crystal clear

that Tornado Cash was specifically set up so that the founders did not transmit funds at all. The undisputed evidence at trial is that Mr. Storm sought to and did create a noncustodial platform that permitted *users themselves* to transmit funds, which meant that no company or business had to act as an intermediary money transmitter. (*See* TFA #1.) The government points to no evidence—and there is none—undermining the founders' clear intent never to take custody or control of users' cryptocurrency and therefore not to "transmit" any funds. Indeed, that was the whole point of Tornado Cash—it was both non-custodial and immutable, meaning there never was, and never will be, any ability for anyone other than the user to have custody or control of the user's cryptocurrency. (*Id.*) The undisputed design of Tornado Cash vitiates any contrary argument about Mr. Storm's intent.

Lacking a shred of evidence of a criminal agreement among the Tornado Cash founders to engage in money *transmitting* at all, the government's opposition advances an improper negligence-based theory by focusing instead on whether the evidence supported an agreement to engage in an *unlicensed* money transmitting business, *i.e.*, a business involving the "transportation or transmission of funds that are known to the defendant to have been derived from a criminal offense." *See* 18 U.S.C. § 1960(b)(1)(C). (*See* Opp. at 55.) The government argues that Mr. Storm's compliance efforts (such as implementing the Chainalysis Oracle) were "half measures" because he observed they were "'easy' to circumvent."[5] (Opp. at 44, quoting *United States v. Ho*, 984 F.3d 191, 199 (2d Cir. 2020).) But the government's repeated reliance on the effectiveness of deterrence measures, or the failure to create a different product along the

[5] The government's characterization of the Chainalysis Oracle as a "phony measure" for "public relations" purposes requires an inferential leap unsupported by the cited discussions. (*See* Opp. at 46.) These were not admissions of insincerity but honest, fearful reflections on its technical limitations—namely, that tech-savvy users could bypass it, a reality acknowledged by experts (*e.g.,* Tr. 1185:24-1187:3 (Werlau); Tr. 1827:22-1828:16 (Edman)).

lines of Mr. Werlau's suggestions, improperly imports a negligence standard into criminal conspiracy.

This Court should find such negligence evidence inadequate as a matter of law to meet the government's burden to prove defendant agreed to a "joint enterprise for a criminal purpose." *United States v. Khalupsky*, 5 F. 4th 279, 288 (2d Cir. 2021). This is particularly true as the government's own evidence failed to elucidate a remedy "any idiot would have known" to implement. (7/8/2025 Tr. 61:24-62:10). Mr. Werlau's "proposals" (Tr. 1157:14-1158:17, 1160:18-21, 1188:12-14) effectively treat Tornado Cash like a financial institution subject to the Bank Secrecy Act—but without explicitly referring to the Act or terms like AML and KYC. Of course, Tornado Cash is not a financial institution, nor does the government argue that it or the founders were obligated to comply with the Act (they obviously were not). Given the absence of a regulatory obligation, the government is left to quarrel with the founders' compliance choices by arguing they had some sort of duty to do more to stop bad actors. But again, this is a negligence theory of liability and cannot be the basis to find a criminal agreement existed to engage in an unlicensed money transmitting business.

The government offered no other evidence. On page 42 of its opposition, the government offers a string cite to Telegram messages, but none of them shows that the founders intended to engage in a *business* involving money *transmitting*, much less an *unlicensed* one. At most, they show generalized knowledge of misuse of the software by bad actors, and concerns about that misuse. Importantly, the government cites no message that undermines the founders' core understanding that Tornado Cash, due to its permissionless and non-custodial nature, (1) did not transmit funds; (2) was not a business (*see infra* Section III.E); and (3) did not transmit illicit funds (because it did not transmit funds at all).

B. The Evidence Failed To Establish Mr. Storm Acted with Willfulness

The evidence adduced at trial was insufficient to show that Mr. Storm *willfully* participated in the conspiracy to operate an unlicensed money transmitter with the intent to achieve the underlying objective. The government's claim to the contrary is belied by its own repeated characterization of Mr. Storm's conduct—that he was aware that illicit actors were misusing the Tornado Cash protocol but did not take adequate steps to prevent such misuse and "continued to take affirmative steps to operate" Tornado Cash. (*See* Opp. at 13, 45, 49-51, 71, 87, 96.) For all the reasons explained in the motion, that is insufficient. (*See* Mot. at 34, 36-43, 62-63, 71-75.)

As this Court instructed the jury, the government was required to prove that "Mr. Storm knowingly and willfully became a member of the charged conspiracy with *the intent to further its illegal purpose*, that is, with the intent to achieve the object of the charged conspiracy." (Dkt. 225 at 45 (Count Two).) These instructions reflect well-established precedent that a willful act in the criminal context "is one undertaken with a 'bad purpose'" and "with knowledge that [the] conduct was unlawful." *Bryan v. United States*, 524 U.S. 184**,** 191-92 (1998) (quotation omitted). "[W]here the crime charged is conspiracy, a conviction cannot be sustained unless the [g]overnment establishes beyond a reasonable doubt that the defendant had the specific intent to violate the substantive statutes." *United States v. Gaviria*, 740 F.2d 174, 183 (2d Cir. 1984) (cleaned up).

Here, the government failed to carry its burden because the evidence showed only that Mr. Storm was aware that certain bad actors were using the protocol and continued to "operate" Tornado Cash without implementing certain novel and speculative features that the government contends would have prevented such illicit use.

1. Mr. Storm's Continued Work on Tornado Cash Does Not Demonstrate Willful Intent To Violate Section 1960

Mr. Storm's continued work on Tornado Cash does not reflect an intent to achieve a criminal purpose because the development or even "operation" of a cryptocurrency mixer was not itself illegal or inherently illicit. Indeed, this Court denied as moot the defense's motion *in limine* to preclude the government from making that argument in light of the government's representation that it would not do so. (*See* Dkt. 173 at 36-37; 7/8/2025 Tr. 125:2-5.) Further, the evidence at most showed that approximately 15% of funds deposited into Tornado Cash during the relevant period could be traced to illicit activity. (*See* DX 8785-36.) Yet throughout its opposition, the government repeatedly cites the "affirmative steps" Mr. Storm took "to operate" the Tornado Cash protocol in support of its argument that it established the requisite *mens rea*, as if such steps could only be in furtherance of unlawful conduct. (*See, e.g.,* Opp. at 13 (Mr. Storm "continued to pay thousands of dollars to service providers and employees and incur other expenses").[6] The government cites no authority for its argument that the continued development of otherwise lawful software, combined with general knowledge of some illicit use, is sufficient to establish an intent to further the illicit use. The authorities the government does cite are inapposite or actually undermine its argument. (*See* Opp. at 49-50.)

The government's reliance on *Rosemond v. United States* is misplaced. (*See* Opp. at 49 (citing 572 U.S. 65, 78 n.9 (2014)).) There, to establish intent, the government had to prove the defendant "actively participate[d]" with "foreknowledge" that a gun would be used to commit

[6] *See also id*. at 14 (Mr. Storm "continued to operate and pay for the Tornado Cash website and UI, ensure the reliability of its blockchain traffic through service providers Infura and Alchemy, manage the relayer network, and promote Tornado Cash"); *id.* (he "incurred significant monthly expenses, engaged in marketing," and purportedly "adopted a for-profit business model that monetized the revenue streams obtained from relayer fees"); *id.* at 87 (he "affirmatively acted to keep operating the Tornado Cash business, to keep upgrading it, to pay the various costs associated with the business").)

the drug trafficking crime at issue. 572 U.S. at 77-78. *Rosemond* thus addressed circumstances in which the jury could infer the defendant's *knowledge*, which could in turn be probative of his *intent* only where he "actively participate[d] in the criminal venture"—*i.e.*, where he was at the scene of the crime and saw "a gun was displayed or used by a confederate." *Id*.

Here, Mr. Storm's general efforts to continue development of or even "operate" a lawful software protocol are nothing like a defendant who is present at the scene of a robbery, sees a confederate wield a gun, and *continues to participate in the robbery*. Mr. Storm did not actively conduct any particular transaction (*see* TFA #1), and could only learn, based on the same public blockchain data available to anyone else, that certain bad actors had deposited funds into the Tornado Cash protocol *after* the fact,[7] which does not show "knowledge at a time [he could] do something with it." *Rosemond*, 572 U.S. at 78. Mr. Storm's later-acquired knowledge of illicit use does not demonstrate an intent to achieve the objects of the money transmitting conspiracy, which ultimately turn on his purported desire to facilitate such illicit use.

Similarly unavailing is *United States v. Dupree*, 2012 WL 5333946, at *24 (E.D.N.Y. Oct. 26, 2012). (*See* Opp. at 50.) The defendant's conduct in *Dupree* of directing and receiving updates on fraudulent accounting entries and sending out false emails to justify them could *only* have been in furtherance of the illicit purpose (bank fraud), whereas here, the mere development or "operation" of Tornado Cash is not itself illicit, and Mr. Storm's efforts equally redounded to the benefit of Tornado Cash's legitimate user base. *Dupree*, 2012 WL 5333946, at *24. And

[7] The government claims Mr. Storm was "capable of informing himself" "which specific transactions each day were the Lazarus Group's deposits, and decided not to." (Opp. at 82.) The evidence does not support this claim. (TFA #4). Given the evidence that bad actors first transferred illicit funds to intermediary wallet addresses before depositing into Tornado Cash, the government does not—and cannot—explain how Mr. Storm could have identified a particular wallet address from which the Lazarus Group—or any illicit actor—was planning to deposit funds into Tornado Cash *before* it conducted that transaction.

again, Mr. Storm had no role in processing Tornado Cash transactions, as Tornado Cash was both noncustodial and permissionless. (*See* TFA #1 and 2).

Mr. Storm's role is more analogous to the defendants in *Smith & Wesson* and *Twitter*. (*See* Mot. at 61-62 (citing *Smith & Wesson Brands, Inc. v. Estados Unidos Mexicanos*, 605 U.S. 280, 292 (2025); *Twitter v. Taamneh*, 598 U.S. 471, 503 (2023)).) The inquiry the Supreme Court articulated and applied in these cases asked whether the defendant "consciously, voluntarily, and culpably participate[d] in or support[ed] the relevant wrongdoing." *Twitter*, 598 U.S. at 505; *see also Smith & Wesson*, 605 U.S. at 291 (inquiring whether defendant "'participate[s] in' a crime 'as in something he wishes to bring about' and seek by his action to make succeed'").

In a recent amicus brief filed by the government with the Supreme Court in a copyright case, the government drew a similar distinction, siding with Cox Communications, an internet services provider whose customers had repeatedly infringed copyrights. *See* Br. for the United States as Amicus Curiae, *Cox Commc'ns, Inc. v. Sony Music Ent.*, No. 24-171 at 23 (Sept. 5, 2025). The government stated that a defendant's "knowledge that a particular buyer plans to mis-use a product with substantial legitimate uses, without more, does not support an inference of the seller's culpable intent" where the defendant "derives income from those users on the same terms that it derives income from non-infringing accounts" because "the continued provision of services at most shows [the defendant's] 'indifference' to infringement" and "does not show that [defendant] culpably intended to participate in infringement or wished to bring it about." *Id.* (quoting *Smith & Wesson*, 605 U.S. at 297).

The same principles should apply in assessing whether Mr. Storm "knowingly and willfully became a member of the charged conspiracy with the intent to further its illegal

purpose." (*See* Dkt. 225 at 29; *Gaviria*, 740 F.2d at 183.) The government's cited evidence demonstrates Mr. Storm's efforts to continue the development and operation of Tornado Cash generally, with no indication that such efforts were directed at bad actors to support or promote their illicit conduct or otherwise "make it his own," and only showed, at most, an "indifference" to the misuse that does not demonstrate culpable intent. (*See* Opp. at 13, 14, 87.)

2. Evidence Regarding Purported Lies to Victims and Mr. Storm's Failure To Implement a User Registry Do Not Demonstrate Willfulness

The other "affirmative conduct" the government relies on consisted of "lying to victims about [Mr. Storm's] degree of control over Tornado Cash and lying to the public about Tornado Cash purportedly 'blocking' North Korean transactions." (Opp. at 75 (addressing Count One).) Again, the government's argument is vitiated by the design of Tornado Cash itself—*i.e.*, non-custodial (meaning no control over victim's funds), permissionless (meaning anyone could use it), and immutable (meaning no one could prevent North Koreans from using it). (*See* TFA #1, 2.) Moreover, as explained above, Mr. Storm's statements about the degree of control he had over Tornado Cash were made in response to inquiries from victims of hacks seeking ways to get their stolen funds back, and nothing he said in response was untrue—it is undisputed that no one except the user with the private note could exercise any custody or control over funds deposited to or withdrawn from Tornado Cash. (*See* TFA #1; *supra* Section III.A.)

Finally, Mr. Storm's failure to implement a feature akin to Mr. Werlau's proposed user registry does not reflect willfulness or a culpable state of mind. Werlau's novel proposal improperly treats Tornado Cash like a financial institution and was far from an easy and obvious fix that Mr. Storm should have and easily could have implemented, as the government promised pretrial. (TFA #7). Recognizing this shortcoming, the government now states that the proposed fix "was hardly the cornerstone of the [g]overnment's case." (Opp. 50.) But the government's

other evidence consisted merely of Mr. Storm's general awareness that bad actors were misusing the protocol, his efforts to continue developing and "operating" Tornado Cash, and his statements that the government characterizes as lies but, even in the light most favorable to the government, were truthful statements in response to inquiries about Mr. Storm's ability to help victims get their stolen funds back. (*See, e.g.,* Opp. at 9, 23-24, 50, 71, 75.) The government ultimately failed to adduce sufficient evidence of Mr. Storm's willful participation in the money transmitting conspiracy with the intent to achieve the underlying object.

C. There Was No Evidence That Mr. Storm Knew That Tornado Cash Was a Money Transmitting Business

As it did at trial, the government fails to meaningfully address an essential element of Count Two—that Mr. Storm *knew* that Tornado Cash was a money transmitting business. *See United States v. Elfgeeh*, 515 F.3d 100, 133 (2d Cir. 2008). The government instead seems to confuse the knowledge issue with the issue of whether Tornado Cash was legally a money transmitting business. (*See* Opp. at 56.) But the government was required to prove *both* that Tornado Cash was such a business *and* that Mr. Storm knew it. *See id.* (Section 1960 requires "proof that the defendant *knew* that the business was engaged in money-transmitting") (emphasis added)); (Dkt. 225 at 46-47 (government required to prove that "Mr. Storm or a co-conspirator controlled, conducted, managed, supervised, directed, or owned all or part of that busines*s with knowledge that it was used as a money transmitting business*" (emphasis added).)

The government also obfuscates the issue by arguing that the Section 1960(b)(1)(C) definition of money transmitting business is different from the Section 1960(b)(1)(B) definition and that only the latter incorporates the definition contained in 31 U.S.C. § 5330(d). (*See* Opp. at

55.) This definitional debate is irrelevant to Mr. Storm's knowledge.[8] In fact, the evidence failed to show that Mr. Storm knew that Tornado Cash was a money transmitting business, under either definition. The government points to a few references in the record to "transactions" and "transfers" of funds. (Opp. at 57.) But none of these references undermine the premise that Mr. Storm believed that it was only *users* who transferred funds using Tornado Cash as a tool, given that Tornado Cash was a noncustodial piece of software.

The government also attempts to show knowledge by pointing to the founders' control over certain elements of the "Tornado Cash service," namely the router and the UI. (Opp. at 57.) But the ability to *control* (*i.e.*, make changes to) either piece of software does not mean that the founders ever had *control* over a user's crypto assets, which is the relevant inquiry. It is undisputed that they did not. (*See* TFA #1).

Accordingly, that Tornado Cash was noncustodial is not "irrelevant" (*see* Opp. at 60), but critical—not only to the legal analysis, but also to Mr. Storm's understanding of what it meant to operate a money transmission business. Notably, although the government quibbles with the evidence Mr. Storm cited demonstrating his belief that Tornado Cash was not a money

[8] In any event, as Mr. Storm has previously argued, the definition of a money transmitting business must be consistent throughout Section 1960. (*See* Dkt. 30 at 25-26.) Indeed, *United States v. E-Gold, Ltd.*, 550 F. Supp. 2d 82, 92 n.10 (D.D.C. 2008) expressly acknowledged that "there is virtually no substantive difference, nor did Congress intend there to be a substantive difference, between the terms 'money transmitting' in Section 1960 and 'money transmitting business' in Section 5330." *Id.* The government's reliance on *United States v. Mazza-Alaluf,* 621 F.3d 205, 210 (2d Cir. 2010), is misplaced. (Opp. at 55.) There, reviewing under the plain error standard, the Second Circuit considered whether a money transmitting business, for purposes of a Section 1960(b)(1)(A)charge, is required to be a "domestic financial institution" subject to 31 U.S.C. § 5313's reporting requirements. *Id.* at 209. Whether Tornado Cash was a domestic financial institution is not at issue here. Further, the Second Circuit's discussion of 31 U.S.C. § 5330(d) was *dicta*, given that it found that the business was a domestic financial institution. *Id.* at 210-11.

transmitting business, it cites no other evidence bearing on Mr. Storm's knowledge, other than the Medium post that described Tornado Cash as providing "noncustodial anonymous transactions on Ethereum" (GX 1901), which only further demonstrates Mr. Storm's belief in the relevance of Tornado Cash's noncustodial nature. Thus, even if this Court concludes that a noncustodial software protocol can be a money transmitting business, it should acquit Mr. Storm because the government introduced no evidence that Mr. Storm knew that.[9]

D. The Evidence Failed To Establish the Requisite Knowledge of the Transmission of Criminal Proceeds

Tellingly, the government never contends that Mr. Storm had any knowledge, prior to the funds' transmission, that the specific funds transmitted were derived from criminal activity. Instead, the government argues that it is sufficient that Mr. Storm had general knowledge that criminals had used Tornado Cash to conceal proceeds in the past. (Opp. at 60-61.) The government's interpretation ignores the statute's plain language, which states that an unlicensed money transmitting business includes one that "otherwise involves the transportation or transmission of funds *that are known* to the defendant to have been derived from a criminal offense." 18 U.S.C. § 1960(b)(1)(C) (emphasis added). The statute's use of the word "that" limits the unlawful transmission to only those funds *that are known* to the defendant, at the time of transmission, to have been derived from criminal activity. The statute does not say, as the government would have it, that it is illegal to transmit *any* funds once the defendant becomes aware that some criminals have transmitted criminally derived funds in the past.

[9] The government also quibbles with the defense's reliance on the FinCEN Guidance as requiring control over the funds. (Opp. at 59 n.16.) *See* FinCEN, FIN-2019-G001, *Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies* (May 9, 2019) ("FinCEN 2019 Guidance"), § 4.2. While this Court has interpreted the FinCEN Guidance differently, a reasonable layperson such as Mr. Storm certainly could have understood that control of funds is required for a software protocol such as Tornado Cash.

Nor would such an interpretation be reasonable. Under the government's scenario, a Western Union operator could be criminally liable for continuing to wire perfectly legal funds as soon as the operator learned that some criminal had at some past point used Western Union to wire criminally derived funds. Congress surely did not intend such a sweeping result. The government cites no law mandating that developers abandon open-source privacy tools due to third-party misuse. Indeed, in *Twitter*, the Supreme Court rejected just such a sweeping theory of liability in the analogous context of social media platforms' liability for misuse. *See* 598 U.S. at 503 (rejecting effort to "effectively hold [a general services] provider liable for . . . wrongdoing merely for knowing that the wrongdoers were using its services and failing to stop them").

The government claims that *United States v. Sterlingov* "rejected the same argument." (Opp. at 61 (citing 573 F. Supp. 3d 28, 35 (D.D.C. 2021)).) But *Sterlingov* was merely a detention order that described the "nature and circumstances of the offense" as the government had charged them in the indictment; the district court did not address what constituted sufficient evidence under Section 1960(b)(1)(C), much less address whether Sterlingov had (or was required to have) knowledge that the specific funds being transferred were criminally derived. *Sterlingov*, 573 F. Supp. 3d at 34-35.

Nor does the fact that this is a conspiracy charge change the knowledge requirement. (*See* Opp. at 61-62.) While it is true that no transfers actually had to be completed, Mr. Storm still had to have conspired to transmit funds *that were known* to him to have been derived from criminal activity. *United States v. Feola*, 420 U.S. 671, 695 (1975) ("the knowledge of the parties is relevant to the same issues and to the same extent as it may be for conviction of the substantive offense"); *United States v. Tavoularis,* 515 F.2d 1070, 1074 (2d Cir. 1975) (to be guilty of

conspiracy, defendant must have the same knowledge required for the substantive offense); *see also infra* at Section IV.C (collecting cases). Here, Mr. Storm had no such knowledge.

E. The Evidence Was Insufficient To Prove that Tornado Cash Was a Money Transmitting "Business"

While recognizing that this Court has previously ruled otherwise, the defense maintains its view that Tornado Cash cannot be considered a money transmitting business for purposes of Section 1960 because it did not charge a fee, as required by Second Circuit case law. *See United States v. Velastegui,* 199 F.3d 590, 592, 595 n.4 (2d Cir. 1999); *United States v. Banki,* 685 F.3d 99, 113 (2d Cir. 2012). The government makes no claim, nor could it, that Tornado Cash charged a fee. Instead, the government relies on "profits derived from fees paid to relayers" to show that Tornado Cash was a business. (*See* Opp. at 63.) First of all, the government's claim exceeds its proof. There was no evidence that there were "profits derived from fees paid to relayers." At most, the government proved that, through the relayer registry, "defendant hoped to profit from TORN through these means." (*Id.*) The tacit admission is that Mr. Storm did not in fact profit from the relayer registry, as the evidence showed. (Tr. 2083:11-22 (Hurder).)

The government further overlooks that any "profits" derived from relayer fees would have been in the form of increased value of TORN tokens, which were the profits of TORN holders, not of Tornado Cash. Tornado Cash itself generated no revenue and continues to operate to this day as open-source software, without any involvement from the founders and without generating any revenue. (*See* Tr. 761:18-23 (Galano); Tr. 2044:21-23 (Hurder).) Any indirect TORN token value appreciation stemmed from market dynamics and governance (Tr. 2075:7-

2076:8, 2081:3-7 (Hurder)), not "profits" from the transmission of funds. This indirect appreciation in assets does not transform Tornado Cash into a "for-profit" business.[10]

Finally, the government points to other evidence—such as having a CEO and soliciting investment from a venture capital firm—to establish that Tornado Cash was a business. (Opp. at 64-65.) But these were the activities of Peppersec, not Tornado Cash. Peppersec was not even alleged to be a money transmitting business; nor could it be, as it never engaged in any transmission of money. Tornado Cash, the only relevant entity here, was a free, publicly available software tool, not a business.

F. The Evidence Did Not Establish That the Founders Transferred Funds in Any Way

The evidence also failed to establish a violation of Section 1960 because it failed to establish that the alleged co-conspirators "transferred" any funds. Even assuming arguendo that a "transfer" could occur without custody or control (a proposition with which Mr. Storm disagrees), a "transfer" clearly must involve at a minimum the actual movement of funds. (*See infra*, Section IV.B.) Under any understanding of the word "transfer," the founders did not themselves transfer any funds.

The government nevertheless maintains that certain aspects of Tornado Cash that the founders controlled, including the UI, "transferred" funds. (Opp. at 65-66.) While not contesting that the UI did not write deposit transactions to the blockchain, the government contends that the UI was "still conducting the transaction; it [was] just using the user's wallet software as a tool to implement the transaction." (Opp. at 66.)[11] This contradicts the evidence and is simply wrong:

[10] While the government states that returns from any business venture become "personal" once earned (Opp. at 64 n.19), the opposite is not true; personal returns do not become business ones. Here, the fact remains that Tornado Cash is the alleged "business" and never generated returns.

[11] The government uses the words "transaction" and "transfer" interchangeably throughout this section, but the operative words under Section 1960 are "transfer" and "transmit." The word

the UI communicated with the software for the user's wallet, where the digital assets were stored, and it was indisputably the user's wallet software that effectuated the transfer on the blockchain. (*See, e.g.*, TFA # 6).

The government also argues that *withdrawals* were effectuated by the UI, claiming that it "wrote the instructions and delivered them to a relayer, which then communicated them to the blockchain," from which the government concludes that withdrawals "are performed exclusively by Tornado Cash, not the user's wallet." (Opp. at 65-66.) This argument assumes that relayers were part of the Tornado Cash protocol or otherwise under the control of Mr. Storm and his co-conspirators. However, it is undisputed that relayers were independent third parties who set and collected their own fees, which were not shared with the founders. (*See* TFA #5).

G. Money Transmitting Requires Custody or Control of the Funds, and Evidence of Such Custody or Control Was Indisputably Absent

The government does not address Mr. Storm's argument that custody or control over the funds is required to be a money transmitter under Section 1960, except to say that this Court has already decided the issue. (*See* Opp. at 56-57.) The defense, of course, recognizes that this Court has previously ruled on the issue and will not repeat its briefing here, but this Court remains free to reconsider its previous ruling, particularly after considering the evidence presented at trial.

It is worth pointing out that the government never contends that the founders had custody or control of the funds. Nor could it. The evidence was undisputed that Tornado Cash was noncustodial, *i.e.,* it never took custody of the users' funds. (*See* TFA #1).) Neither the founders nor the UI ever took custody of the funds because they did not have access to the secret note;

"transaction" is relevant for the Section 1956 analysis below, where it is defined by statute. For this reason, Mr. Storm will focus on the transfer.

only the user did. (Tr. 1147:19-20; 1193:24-1194:1; 1198:15-1199:5 (Werlau); Tr. 1750:21-1751:1; 1807:4-8, 1809:5-6 (Edman).)

The government does argue that the founders had "control" over certain features of Tornado Cash, namely the UI and the router. (*See* Opp. at 57-58.) As discussed above, the government is playing a semantic game, emphasizing "control"—meaning the ability to change—the UI or router software, when the control that matters is the ability to control a user's digital assets, which the founders never had. At all times, Tornado Cash was a non-custodial and user-controlled agnostic piece of software. It is indisputable that neither the founders nor the Tornado Cash tools ever had custody or control over the *funds* being transferred, which is what was required to be deemed a money transmitter under Section 1960.

H. Subsection (b)(1)(C) Does Not Apply to Tornado Cash Because It Was Not Registered

The government challenges the defense argument that subsection (b)(1)(C) of Section 1960 logically can only be applied to money transmitting businesses that are registered. (*See* Opp. at 67-68.) The government's main line of attack is to revert to its argument that the definition of money transmitting in 31 U.S.C. § 5330(d), while incorporated in subsection 1960(b)(1)(B), is not applicable to subsection 1960(b)(1)(C). (*Id.*) For all the reasons discussed above and in Mr. Storm's motion (*see supra* Section III.C n.8, and Mot. at 58), the government is wrong, and money transmitting must have the same definition throughout Section 1960.

The government is also wrong when it argues that limiting the application of subsection (b)(1)(C) to defendants who are registered would lead to the absurd result that money transmitters would be able to "move unlimited illicit proceeds" if they are unregistered. (*See* Opp. at 68.) The defense's whole point is that any money transmitter is required to register under subsection (b)(1)(B), so any unregistered money transmitter would be subject to prosecution

under subsection (b)(1)(B), and subsection (b)(1)(C) thus becomes superfluous as to unregistered money transmitters.[12] The only time subsection (b)(1)(C) serves a purpose is when a registered money transmitter transfers illicit funds because only then would the government not otherwise be able to charge a registration violation under subsection (b)(1)(B).

IV. THIS COURT SHOULD ENTER A JUDGMENT OF ACQUITTAL ON COUNTS ONE AND THREE

The government has failed to offer sufficient evidence to prove Counts One and Three. As to both counts, the government has failed to prove willfulness. Mr. Storm's willfulness arguments in Section IV(B) equally apply here and are incorporated by reference.

The government also failed to prove a criminal agreement to commit money laundering or sanctions violations. Mr. Storm's arguments addressing the criminal agreement for Counts One and Three overlap, and are therefore combined in subsection A below.

Finally, Count One fails for the additional reasons that the government failed to prove that Mr. Storm agreed that a co-conspirator would (or did) conduct a money laundering transaction, and because the government did not prove the requisite knowledge. Count Three fails for the additional reasons that Mr. Storm did not provide "services" "to" or "for the benefit of" the Lazarus Group, and because the informational materials exception to the IEEPA applies.

A. The Government Did Not Prove a Criminal Agreement To Commit Money Laundering or Sanctions Violations

In its own words, the government's criminal agreement theory is that the founders agreed to "maintain the [Tornado Cash] business and continue its operations, including upgrading the software and finding a way to monetize it, even after they knew that it had become a haven for

[12] Indeed, the government charged Mr. Storm in this very case with conspiring to violate subsection (b)(1)(B). (Dkt. 105.) The government simply elected to forego that theory (Dkt. 144), but it could just as easily have elected to prosecute this case under subsection (b)(1)(B).

hackers, money launderers, and sanctions evaders." (Opp. at 70.) In other words, although, as the government concedes, there was nothing *per se* unlawful about running the "Tornado Cash business" (*id.*), once defendant learned that bad actors were using the Tornado Cash software, defendant had a duty to prevent their use or his lawful agreement can be deemed a criminal one. This does not amount to an agreement with an unlawful or criminal purpose as a matter of law. *See, e.g.*, *United States v. Garcia*, 587 F.3d 509, 515 (2d Cir. 2009) ("Conspiring to launder money requires that two or more people agree to violate the federal money laundering statute").

There is no dispute about the government's theory and the facts it contends support it. This is the exact theory the government set forth in summation, from which it now attempts to distance itself. (*See* Tr. 2341:12-2342:4; Tr. 2442:11-24, 2450:14-2452:1 (rebuttal).) The theory is summarized in the above passage from the Opposition and is fleshed out in detail as to Count Three, where the government contends the following facts are sufficient to support a criminal agreement: (1) when defendant "learned that the Lazarus Group was laundering funds"; (2) "[f]or the next ten days, the defendant . . . continued running the business, taking no steps to prevent the Lazarus Group's transfer of funds through Tornado Cash"; (3) then, after OFAC announced sanctions on April 14, 2022, defendant "[took] the half-measure of implementing the Chainalysis Oracle"; (4) in "ensuing weeks," defendant "discussed the fact that they were still processing transactions" and "continued to engage in these transactions";[13] and (5) ultimately, "the only decisive step the defendant took in response was to secretly start cashing out the founders' TORN tokens in June." (Opp. at 84).[14] These points boil down to what has always

[13] This Court should reject the hyperbole here and in other places of the brief suggesting that Mr. Storm conducted transactions or transmitted funds. The undisputed facts show that he did not. (*See* Mot. at 5-6 (summarizing evidence from Werlau, Bram, Gibbs, Dubash and Edman).)

[14] The government complains that the defense does not "question the overwhelming evidence supporting this theory" (Opp. at 70), but that merely demonstrates deference to the Rule 29

been the government's theory, that, having learned of the bad actors' use of the protocol, the founders adopted inadequate deterrence measures that failed to prevent its misuse, and ultimately sold some personal TORN tokens.

These facts do not to support a criminal conspiracy. To prove a criminal conspiracy, the government was required to show that two or more persons entered into a joint enterprise for an unlawful purpose, with awareness of its general nature and extent. *Khalupsky*, 5 F. 4th at 288. But the government's theory is entirely based on the founders having a lawful agreement to build a protocol— or even a "service," or a "business," as the government uses these terms to try to shoehorn in its preferred legal construction—while knowing bad actors were using it and failing to prevent their use.

The government does not engage with any of the caselaw concerning its need to prove that the founders had an agreement with an unlawful or criminal purpose. In fact, the only citation it provides concerning the conspiracy elements is to *United States v. Henry*, 325 F.3d 93, 103 (2d Cir. 2003) (Opp. at 70), which focuses on the application of the agreement element to the elements of the underlying substantive charge. Of course, to prove an agreement to a criminal object, the government must prove not only a conspiratorial agreement and intent, but also that defendant intended each of the elements of the substantive offense. (*See* Dkt. 225 at 32). The deficiencies in the government's proof as to these elements are discussed below.

But the first element of any criminal conspiracy is the agreement element, that is, that a conspiracy existed. (Dkt. 225 at 28). To meet its burden, the government must show that the

---

standard. While Mr. Storm disputes the government's evidence underlying the "business" and "monetiz[ation]" claims, this Court need not resolve them for purposes of determining whether the government has presented sufficient evidence of a criminal agreement. Even permitting the government the factual inferences in its favor, these facts do not support an unlawful agreement.

agreement at issue had an unlawful or criminal purpose. *See Pettibone v. United States*, 148 U.S. 197, 203 (1893) ("the criminality of a conspiracy consists in an unlawful agreement of two or more persons to compass or promote some criminal or illegal purpose"); *Blumenthal v. United States*, 332 U.S. 539, 558 (1947) (conspirators are joined by a "common plan" and a "common single goal"); *Garcia*, 587 F.3d at 515 ("unlawful or criminal purpose").

The government cannot meet its burden to show an unlawful or illegal purpose by combining innocuous acts to continue Tornado Cash, or even make money on it, coupled with knowledge of bad actors' misuse of it. As the Second Circuit has explained, "in prosecutions for conspiracy … [i]t is not enough that [the defendant] does not forego a normally lawful activity, of the fruits of which he knows that others will make an unlawful use; he must in some sense promote their venture himself, make it his own, have a stake in its outcome." *United States v. Falcone*, 109 F.2d 579, 581 (2d Cir. 1940), *aff'd*, 311 U.S. 205 (1940).

Notably, *Falcone* was cited in *Smith & Wesson*. *See* 605 U.S. at 292. Dismissing *Smith & Wesson* and *Twitter*, 598 U.S. 471 (2023), as civil cases, the government claims it is "not seeking to hold [Mr. Storm] derivatively liable for substantive crimes committed by others." (Opp. at 76 n.22). In fact it is, given that the only persons who committed the substantive crime of money laundering were the bad actors.

Further, *Smith & Wesson* and *Twitter* expressly apply criminal law (*see* 605 U.S. at 287, 598 U.S. at 488, respectively)—not only principles of aiding and abetting liability but also conspiracy principles. In *Twitter*, expressly citing a criminal treatise, the Supreme Court explained that "our legal system generally does not impose liability for mere omissions, inactions, or nonfeasance; although inaction can be culpable in the face of some independent duty to act, the law does not impose a generalized duty to rescue." 598 U.S. at 489. In *Smith &*

Wesson, citing not only *Falcone* but also conspiracy cases such as *Direct Sales Co. v. United States*, 319 U.S. 703, 711, (1943), the Supreme Court provided guidance on how to determine whether a criminal purpose exists, concluding that a "merchant becomes liable only if, beyond providing the good on the open market, he takes steps to 'promote' the resulting crime and 'make it his own.'" 605 U.S. at 292 (quoting *Falcone*, 109 F.3d at 581).

Against these authorities, the government's factual proffer falls far short of evincing a criminal agreement, as Mr. Storm made no efforts to support or promote the illicit conduct of bad actors or otherwise "make it his own." The government offers five categories of facts:

First, the government cites the evidence that the protocol was used by bad actors, and that the founders learned of it, and discussed it. (*See* Opp.at 71-21 ("sheer volume of the laundered funds"; "repeated communications . . . notifying [founders] that their business was concealing dirty money"; and "internal communications about dirty money being laundered"). This evidence is indisputably at the crux of their case, but it is insufficient to establish a criminal agreement.

Second, the government cites Mr. Storm's so-called "consciousness of guilt" (Opp. at 71-72), but this evidence cannot supply the missing element of a criminal agreement here or in any case. It is beyond cavil that "[a]fter the fact 'consciousness of guilt evidence' is insufficient as matter of law to sustain a conviction." *United States v. Cassese*, 290 F. Supp. 2d 443, 454 (S.D.N.Y. 2003), *aff'd*, 428 F.3d 92 (2d Cir. 2005). This is because "feelings of guilt, which are present in many innocent people, do not necessarily reflect actual guilt." *Id.* (citing *Miller v. United States*, 320 F.2d 767, 773 (D.C. Cir. 1963)).[15]

[15] This Court should reject the government's claim that Mr. Storm's communications with Rho bank evince either falsity or a consciousness of guilt. (Opp. at 71-72). The government here reaches far beyond any reasonable inference from the evidence. The government's claim is

Third, the government cites the fact that the founders profited from sales of TORN tokens. (Opp. at 72.) This is a neutral fact, fully consistent with the founders supporting a lawful software "business," particularly as there was no evidence that the TORN profits had any nexus to the alleged criminal use of Tornado Cash. (Indeed, the undisputed evidence was that the TORN price decreased after the Ronin Hack. (Tr. 2030:23-24, 2083:2-8 (Hurder).)[16]

Fourth, Mr. Storm did not "[lie] to victims about his degree of control over Tornado Cash." (Opp. at 71; *supra* Section III.A.) Nor did he "[lie] to the public about Tornado Cash purportedly "blocking North Korean transactions." (Opp. at 71; *supra* Section III.B.2.) This Court is not required to accept specious inferences. *See United States v. Valle*, 807 F.3d 508, 515 (2d Cir. 2015).

In any event, what the government claims defendant lied about was his ability to implement a more effective remedy. Setting aside the government's failure to prove such a remedy, even if Mr. Storm had been in possession of a better option to stop the bad actors from

---

wholly refuted by the spreadsheet itself (GX 923), in which Mr. Storm disclosed, on behalf of Peppersec, that it (1) worked on "open sourced defi projects"; (2) that it received investments in cryptocurrency; (3) that it received "donations, payments and expenses" in cryptocurrency such that to determine the portion of its revenue in cryptocurrency it would need an accountant to calculate; (4) upon receiving a follow up question from Rho, Mr. Storm provided the fact that Peppersec raised money through the crowdfunding site Gitcoin, which itself referenced Tornado Cash information for the software development on the crowdfunding site, which in turn provided detailed information about the Tornado Cash project. (*See* GX 919). In sum, the claim that Mr. Storm's response to a routine bank questionnaire was false or misleading requires an inferential leap. Further, given that the evidence showed Mr. Storm was and has always been very publicly associated with Tornado Cash (Tr. 756:12-757:1 (Gallano); Tr. 1870:25-1871:2 (Edman), the claim rings particularly hollow.

[16] Indeed, the government's evidence fails to tie TORN profits to the protocol use at all. The government asserts (1) that the relayer registry "connected the relayer fees . . . to the value of TORN tokens," (2) that Mr. Storm hoped to profit from TORN through this connection, and (3) that appreciation in the value of TORN would have profited him. (Opp. at 63). The conditional voice is telling, as the government effectively admits that Mr. Storm did not in fact profit from any TORN appreciation due to the relayer registry. Dr. Hurder further disproved any tie between the use of the protocol and the price of TORN. (Tr. 2081:8-2084:7, 2088:7-2089:11.)

accessing Tornado Cash, the failure to implement it to prevent third-party conduct simply does not equate to an agreement to promote the unlawful acts of others and make them his own. As the Supreme Court found in *Twitter*, inaction is not actionable without an independent duty to act. 598 U.S. at 489. The government effectively admits this, in attempting to distance itself again and again from a case based on a negligent failure to act. (*See* Opp. at 3, 45-50, 74).

Fifth, the government attempts to prove a criminal agreement based on: (1) the T-shirt depicting a washing machine; and (2) the 1-inch "free advertising" message (GX 2007-T). (Opp. at 72-73.) Neither of these demonstrates a meeting of the minds to further a criminal purpose. The 1-inch Telegram message was written by a third party, not Mr. Storm, who himself noted that he was "just messing with" Mr. Storm. (GX 2007-T). As this Court well knows, the government's evidence regarding the T-shirt fell flat when the evidence showed it only worn once at a legitimate conference at Harvard in 2019. Moreover, even the government does not contend that the conspiracy began when the founders developed the software back in 2019. Based on the indictment and DeCapua's testimony, the government does not allege that any conspiracy began until the founders were on notice of dirty money going through Tornado Cash, the first instance being in September 2020. (GX-3002-2; Tr. 559:22-560:3 (DeCapua)). Thus, there is zero evidence that, during the alleged conspiracy, the founders "knew that the Tornado Cash service was, first and foremost, a money laundering business and embraced it." (Opp. at 72).

Accordingly, permitting all inferences in favor of the government, the government's evidence of agreement was to: "maintain the business," "upgrad[e] the software" and attempt to "monetize it," after learning that Tornado Cash had become a "haven" for bad actors. (Opp. at 70). Even if one were to add to this list the failure to implement an effective remedy while lying

about it, this conduct falls squarely into what *Falcone* rejects as insufficient to show a criminal conspiracy, as, at most, the defendant failed to "forego a normally lawful activity, the fruits of which he [knew] that others [would] make an unlawful use," but did not "promote their venture himself, [and] make it his own, hav[ing] a stake in its outcome." 109 F.2d at 581.

B. There Was No Evidence that Any Co-conspirator Agreed to Conduct a Money Laundering Transaction

There is overwhelming authority—to which the government does not respond—holding that conspiracy liability makes a defendant vicariously responsible only "for the substantive illegal acts of his co-conspirators, done in furtherance of the conspiracy." *United States v. Head*, 546 F.2d 6, 10 (2d Cir. 1976); *United States v. Piampiano*, 271 F.2d 273, 275 (2d Cir. 1959) ("act of one conspirator is imputed to the other conspirators"); *see also United States v. Rosenblatt,* 554 F.2d 36, 39 (2d Cir. 1977) ("A conspirator's liability *for substantive crimes committed by his co-conspirators* depends on whether the crimes were committed 'in furtherance of the unlawful agreement or conspiracy.'") (citing *Pinkerton v. United States,* 328 U.S. 640, 645 (1946)) (emphasis added)). Indeed, as the Supreme Court explained in *Twitter*, a "significant limiting principle" of conspiracy liability, as distinguished from aiding and abetting liability, is that it requires an "agreement *with the primary wrongdoer* to commit wrongful acts." 598 U.S. at 489-90 (emphasis added).

Conspiracy liability is a form of vicarious liability analogous to a partnership. As the Supreme Court held in *Pinkerton*: "A conspiracy is a partnership in crime." 328 U.S. at 644; *see also* Dkt. 225 at 30 ("when people enter into a conspiracy, they become agents or partners of one another in carrying out this crime."). As *Pinkerton* further explained, "so long as the partnership in crime continues, the partners act for each other carrying it forward" such that "an overt act of one partner may be the act of all[.]" 328 U.S. at 646-47 (citation omitted). For example, "[a]

scheme to use the mails to defraud, which is joined in by more than one person, is a conspiracy. . . [y]et all members are responsible, though only one did the mailing." *Id.* (citation omitted); *see also Salinas v. United States*, 522 U.S. 52, 63-64 (1997) ("The partners in the criminal plan must agree to pursue the same criminal objective and may divide up the work, yet each is responsible for the acts of each other") (citing *Pinkerton* at 328 U.S. at 646); *Ocasio v. United States*, 578 U.S. 282, 288 (2016) (the crime of conspiracy requires a defendant to "reach an agreement with the 'specific intent that the underlying crime *be committed*' by some member of the conspiracy") (citation omitted) (emphasis in original); *United States v. Collazo*, 984 F.3d 1308, 1320 (9th Cir. 2021) (money laundering conspiracy conviction requires proof that "the defendant agreed with another person that some member of the conspiracy would commit the relevant underlying offense"); *Blumenthal*, 332 U.S. at 558 (although defendant salesman "did not know, when they joined the scheme," the identity of all the co-conspirators "or exactly the parts they were playing in carrying out the common design and object of all," they "became parties to the larger common plan, joined together by their knowledge of its essential features and broad scope, though not of its exact limits, and by their common single goal").

By contrast, here, the government is seeking to try to hold Mr. Storm criminally liable for the actions of those who it acknowledges had their own criminal goals and were not joined in a single common goal. It cites no caselaw—and the defense is aware of none—that would support such a broad theory of conspiracy liability. Indeed, other than dismissing Mr. Storm's argument as having been previously rejected at the motion to dismiss stage,[17] the government does not even respond to this argument.

[17] The government asks this Court to "adhere to its prior ruling" but in fact, this Court has not reached this issue, denying Mr. Storm's motion to reconsider on the standard. (Dkt. 127 at 1).

Applying these principles to Count One, this Court should acquit Mr. Storm because the substantive acts of money laundering were conducted by third parties, not co-conspirators or agents of Mr. Storm. Section 1956 (a)(1) provides that, to be guilty of money laundering, a defendant must *conduct* a transaction with illicit proceeds and, at the time the transaction is conducted, must know both (1) that the transaction involved criminal proceeds, and (2) know that the transaction was designed in whole or in part to conceal the proceeds. In the conspiracy context, as discussed further below, while the defendant need not conduct the transactions personally, the defendant must agree, while possessing the requisite knowledge, that a member of the conspiracy (or their agent) will conduct them. But as to Tornado Cash, there is no dispute that the cryptocurrency transactions involving proceeds of specified unlawful activity were conducted by users, not by the alleged co-conspirators.

The government's new argument—that the UI participated in conducting a transaction—is wrong as a matter of law. (See Opp. at 66). The term "financial transaction" and "transaction" are statutorily defined. "Financial transaction" means in relevant part: "a transaction which in any way or degree affects interstate or foreign commerce . . . involving the movement of funds by wire or other means" (18 U.S.C. § 1956 (c)(4)) and the term "transaction" means "a purchase, sale, loan, pledge, gift, transfer, delivery, or other disposition" of such funds (*id.* at (c)(3)). Applied to the technology at issue here, the only relevant definition of transaction is a "transfer" that "involved the movement of funds," *i.e.*, Ether, by wire. Only the transfer of the Ether from one address to another on the Ethereum blockchain is the transaction. (Tr. 1751:18-24 (Edman).) Contrary to the government's bare assertion, the statute itself provides "legal authority" that preparing the code for a transaction and transmitting it over the internet, an action that does not

occur on the blockchain at all, is not a "transfer" "involving the movement of funds," any more than emailing a wire transfer request to the bank is; only the wire transfer itself is the transfer.

The government dismisses out of hand the Second Circuit cases Mr. Storm cites (Mot. 64) which interpret Section 1956 to require that a defendant or their co-conspirator first control the criminal proceeds before conducting a transaction with them. (Opp. at 76-78.) That the cases arise in the "merger" context is not a sufficient basis to reject them, where the Second Circuit's statutory interpretation is instructive. (*Id*.) Specifically, the Second Circuit has found that Section 1956(a)(1) provides a "clearly demarcated" two-step analysis which "requires first that the proceeds of specified unlawful activity be generated, and second that the defendant, knowing the proceeds to be tainted, conduct or attempt to conduct a financial transaction with these proceeds with the intent to promote specified unlawful activity." *United States v. Piervinanzi*, 23 F.3d 670, 680 (2d Cir. 1994); *see also United States v. Napoli*, 54 F.3d 63, 68 (2d Cir. 1995). While the Second Circuit may not have expressly adopted a control requirement in these cases, control is implicit in its "two-step" formulation.

In any event, these cases are wholly consistent with the vicarious liability authorities above, in that they contemplate that a money laundering transaction is one conducted by a defendant or their co-conspirator, which can only happen if the defendant or co-conspirator first gains control of the funds. *See, e.g., United States v. Szur*, 289 F.3d 200, 214 (2d Cir. 2002) (affirming money laundering convictions where funds first entered "the control of the perpetrators" and then were subsequently transferred to other accounts).

Because the government has not proved and cannot prove that Mr. Storm or the alleged co-conspirator founders conspired to conduct any money laundering transaction themselves, this Court should enter a judgment of acquittal as to Count One.

C. There Was No Evidence That Mr. Storm Possessed the Requisite Specific Knowledge

The substantive crime of money laundering requires proof that a defendant, "*knowing* that the property involved in [such] financial transaction represents the proceeds of some form of unlawful activity," *and* "knowing that the transaction is designed" "to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity" "*conducts or attempts to conduct such a financial transaction* which in fact involves the proceeds of [SUA]." 18 U.S.C. § 1956(a)(1) (emphasis added). To be guilty of conspiracy to commit money laundering, Mr. Storm had to have this specific knowledge as well. *Feola*, 420 U.S. at 695; *Tavoularis*, 515 F.2d at 1074; *United States v. Hysohion*, 448 F.2d 343, 347 (2d Cir. 1971) ("the same specific knowledge . . . is also an essential element of the conspiracy to commit such substantive offenses" (quoting *Jefferson v. United States*, 340 F.2d 193, 197 (9th Cir. 1965)); *see also United States v. Molt*, 615 F.2d 141, 146 (3d Cir. 1980) ("when knowledge is an essential element of the underlying substantive offense, it must be proven that all co-conspirators possess the requisite knowledge").[18]

In response to this line of authority, the government offers only inapposite points concerning inchoate conduct (Opp. at 79) and agency liability (*id*. at 80). It is true that conspiracy is an "inchoate offense," *Iannelli v. United States*, 420 U.S. 770, 777 (1975), where a defendant may be convicted "in the complete absence of any transactions" as long he agreed "that such transactions would occur." (Opp. at 79). But here, the government charged an

[18] These authorities follow the Supreme Court's holding in *Ingram v. United States* that a "[c]onspiracy to commit a particular substantive offense cannot exist without at least the degree of criminal intent necessary for the substantive offense." 360 U.S. 672, 678 (1959). For money laundering, Congress made the level of criminal intent and knowledge particularly high, incorporating two elements of knowledge. *See* 18 U.S.C. § 1956(a)(1)(B).

allegedly completed conspiracy in which specific transactions already occurred, so the conditional inchoate language merely distracts from its burden.

Indeed, even if it were a case involving an inchoate offense, where the only issue was whether defendant had entered into a future-facing agreement, the government would be required to prove that the defendant made the agreement to conduct a *specific* transaction while possessing the requisite criminal knowledge. The government mischaracterizes *Henry*, which does not say it is sufficient that the government prove an agreement "with the objective of . . . conducting financial transactions" (*see* Opp. at 70 (citing *Henry*, 325 F.3d at 103)); rather, *Henry* states that the government is required to show "that the defendant agreed to . . . conduct a financial transaction" with the requisite knowledge. 325 F.3d at 103. This requirement is *specific*; that is, while possessing both of the required knowledge elements, the defendant must agree to conduct the transaction. *See also* 18 U.S.C. § 1956(a)(1) (actual knowledge must be possessed at the time "such a . . . transaction" is conducted).

Recognizing that it cannot meet these knowledge requirements with proof of Mr. Storm's specific knowledge, the government responds with cases in which defendants were held vicariously liable for money laundering transactions performed by their agents at their direction. (Opp. at 80). These cases do not assist the government. First, while an individual who directs others to conduct a money laundering transaction can be responsible under a principal-agent theory, there is no evidence that any bad actors who engaged in money laundering transactions were agents of the founders. Second, in both of the cited cases, unlike here, there was no dispute that the defendants knew that the transactions included criminal proceeds at the time they directed their agents to conduct them. *See United States v. Jefferson*, 2009 WL 2447850, at *5 (E.D. Va. Aug. 8, 2009); *United States v. Jackson*, 72 F.3d 1370, 1374, 1385 (9th Cir. 1995);

United States v. Delgado, 256 F.3d 264, 276 (5th Cir. 2001).[19] These cases do not support liability in the absence of the statutorily-required knowledge elements.

Finally, the government turns to the doctrine of conscious avoidance, arguing that it need not prove knowledge because defendant "consciously avoided learning of specific money laundering transactions on Tornado Cash." (Opp. at 81.) But the evidence failed to show any effective way of learning of specific money laundering transactions, other than after the fact, because bad actors could create numerous wallets and quickly hop from one to the other to evade detection. (TFA #4.)[20] Indeed, the only tool to identify and block known transactions by sanctioned entities was the Chainalysis Oracle, which the founders applied to the UI and which did in fact block all sanctioned wallet addresses. Mr. Storm therefore could not have "deliberately avoided confirming [a] fact" (Dkt. 225 at 55) that was not capable of confirmation.

As the Supreme Court has instructed, "evidence of knowledge must be clear, not equivocal" "because charges of conspiracy are not to be made out by piling inference upon inference, thus fashioning what, in [*Falcone*], was called a dragnet to draw in all substantive crimes." *Direct Sales Co*., 319 U.S. at 711. Because the government has no evidence to satisfy the two knowledge elements Congress built into Section 1956, this Court should enter a judgment of acquittal as to Count One.

---

[19] The same distinctions are present in this Court's hypothetical regarding the restaurant business. (7/12/2024 Tr. 57:8-17.) This Court's hypothetical posited an express meeting of minds between the restaurant owner and an individual who was both a money laundering co-conspirator and the perpetrator of the underlying crime. The restaurant owner's agreement with the individual to conduct transactions involving the proceeds of specified unlawful activity for the purpose of concealment satisfies both elements of knowledge. The restaurant owner and the individual then would be responsible under either conspiracy liability or principal-agency liability for the acts of their subordinates in conducting the specific laundering transactions. None of these facts is present in this case.

[20] Even Werlau's hypothetical compliance proposals did not purport to expressly identify potential money laundering transactions in advance.

D. There Was No Evidence that Mr. Storm Provided a "Service" to the Lazarus Group

The government's "ample evidence" supporting Count Three is anything but. It consists of Mr. Storm's allegedly learning of a hack by Lazarus Group and purportedly "taking no steps to prevent the [group's] transfer of funds through Tornado Cash." (Opp. at 84.) In the next breath, the government admits this is overstatement because Mr. Storm implemented the Chainalysis Sanctions Oracle which, even in the government's view, constitutes at least a "half measure."[21] *Id.* Tellingly, even though the Supreme Court has held that the term "service" "refers to concerted activity," *Holder v. Humanitarian L. Project*, 561 U.S. 1, 23 (2010), the government identifies no evidence (because there is none) of communications between Mr. Storm and the Lazarus Group, an agreement between them, or compensation from the Lazarus Group to Mr. Storm. Given the absence of *any* concerted activity between the defendant and the sanctioned entity, the government advances an overbroad, negligence-based view of IEEPA liability that has *never* been used in *any* prior prosecution on record nor approved by *any* court. (*See* Mot. at 73-74.)

Already on the thinnest of ice, the government's argument falls through completely under the weight of *Van Loon v. Department of the Treasury*, 122 F.4th 549 (5th Cir. 2024). Try as it might, the government cannot escape *Van Loon's* import as the definitive appellate court ruling on the Tornado Cash pool smart contracts—a ruling that eviscerates the government's "service" argument by concluding that the smart contracts did not constitute "services" under the IEEPA.

[21] The Chainalysis Sanctions Oracle was 100% effective to block transactions involving wallet addresses that OFAC attributed to Lazarus Group. (TFA #3.) The government cites no authority that obligated Mr. Storm to undertake extensive, burdensome monitoring efforts to ensure no funds attributable to the Lazarus Group could ever be deposited into the pools. (*See Twitter*, 598 U.S. at 489 ("although inaction can be culpable in the face of some independent duty to act, the law does not impose a generalized duty to rescue.").)

Id. at 570. In abrogating the Treasury Department's sanctions on the Tornado Cash smart contracts, the *Van Loon* court noted that they "are nothing more than lines of code" and "are less like a 'service' and more like a tool that *is used in performing* a service." *Id*.

While not disputing this central holding, the government tries to circumvent it by arguing that other features associated with Tornado Cash, like the UI, are services. But the gravamen of Count Three is the alleged misuse of pool smart contracts by the Lazarus Group to purportedly launder cryptocurrency—any purported laundering would be impossible without those smart contracts. *Van Loon* says that if the Lazarus Group did this, then they were availing themselves of a tool, not a service, and the IEEPA has no application. This ends the analysis because the government has not and cannot identify any evidence that the ancillary features of the Tornado Cash protocol were provided as services to or for the benefit of the Lazarus Group.

It is true that this Court contemplated the possibility that the government could prove "that Defendant conspired to violate IEEPA by means of features over which he had control," including the "user interface," the "relayer algorithm and a related relayer registry," or that he "deliberately implemented an ineffective sanctions screen." (Opp. at 88-89.) But the government was still required to prove that Mr. Storm provided a service, and it fails to explain how the other features it identifies—the "website and UI"; the "command line interface"; "the relayer registry"; "TORN tokens"; and "a variety of additional smart contracts, including the router"(Opp. at 89) are anything more than tools used in performing a service rather than being services themselves.

The UI was, like the pool smart contracts, both permissionless and noncustodial, meaning anyone could use it to conduct their own transactions. (*See* TFA #1 and #2). The relayer registry operates automatically via smart contract. (*Id*. #7; Mot. at 7) The CLI and TORN tokens are software code, not services. (*See* Tr. 1783:12-24 (TORN is an ERC-20 token whose functionality

is implemented by smart contract (Edman)); Tr. 1810:11-25 (Edman explaining CLI code); DX 8788 (CLI source code).) Thus, the other features identified by the government are tools, which explains why the government cannot explain how Mr. Storm's ability to change those features equates to the provision of services to the Lazarus Group.

If there were any remaining doubt about the invalidity of the government's theory, *Banki* removes it. The government focuses on *Banki*'s fee component but ignores the facts central to its holding. (*See* Opp. at 89; Mot. at 78.) Unlike this case, the "service" in *Banki* involved a defendant who was in constant communication with sanctioned entities that were the beneficiaries of the service. There, the defendant's family first "*retained the services* of . . . a Tehran-based hawaladar," a hawala broker who used his network to facilitate funds transfers from the defendant's Iranian family to the defendant. *Banki*, 685 F.3d at 103-04 (emphasis added). The defendant sent emails confirming receipt of funds to his family in Iran, who would communicate there with the hawaladar. *Id.* at 104. There was an ongoing relationship between the hawaladar and the defendant and his family—the defendant understood that deposits into his U.S.-based account were part of a scheme to facilitate money transfers to Iran, a service which was not made available to the general public, but that "operate[d] in large part on trust"; and the defendant benefitted: his family sought to transfer funds from Iran to the U.S. "to protect the family's assets." *Id.* at 103-04. The government's overemphasis on the fee issue ignores that the basis for the *Banki* court's affirmance that a service existed was this web of intentional communications and relationships among the hawala brokers and beneficiaries, which is simply not present here.

The government concludes by arguing that, among the examples listed in the North Korea Sanctions Regulations and Iran Sanctions Regulations, Tornado Cash "fits squarely within

one of those examples: financial services" (Opp. at 90-91), but this argument fails for the same reason—Tornado Cash and the ancillary features are tools, not services, which means they do not satisfy the "service" part of the term "financial service." Moreover, OFAC regulations include examples of financial services that contemplate some service provider-customer relationship (which is lacking here). *See* 31 C.F.R. § 510.307 ("The term financial services includes loans, transfers, accounts, insurance, investments, securities, guarantees, foreign exchange, letters of credit, and commodity futures or options."); *see also Matter of Seizure and Search of Motor Yacht Tango*, 597 F. Supp. 3d 149, 172 (D.D.C. 2022) (stating that a sanctioned Russian Oligarch who wired funds via a front company through a U.S. bank violated the IEEPA by causing the bank to export financial services to a sanctioned entity). Both *Banki* and the implementing regulations thus support a definition of "services" that requires some relationship with the recipient of the services, and there was no evidence of any relationship or even communication with the Lazarus Group here. At bottom, the government points to *no case* like this one, because no court has previously entertained such an overbroad theory. This Court should not entertain it either.

E. The Evidence Failed to Show that Mr. Storm Provided Services "To" or "For the Benefit of" the Lazarus Group

Next the government mischaracterizes Mr. Storm's argument about the plain meanings of "to" and "for the benefit of." (*See* Opp. at 91-92.) Whether or not the purported "services" were "also provided to others" (Opp. at 91), the government still must prove that they were provided to or for the benefit of a sanctioned entity. Mr. Storm argues, and the evidence shows, that in developing and continuing to work on permissionless and noncustodial software available to anyone, he was not providing that service *to* the Lazarus Group.

Indeed, the government fails to point to any evidence of any service provided *by* Mr.

Storm *to* Lazarus Group under the plain meaning of those terms. In construing a statute prohibiting the provision of material support to terrorist organizations, including the provision of "services," the Supreme Court noted that the term "service" "refers to concerted activity," and quoted a dictionary definition of the term as "the performance of work commanded or paid for by another: a servant's duty: attendance on a superior"; or "an act done for the benefit or at the command of another[.]" *Humanitarian L. Project*, 561 U.S. at 23-24 (quoting Webster's Third New International Dictionary 2075 (1993)). The Supreme Court found that "[t]he use of the word 'to' indicates a connection between the service and the foreign group," and concluded that "a person of ordinary intelligence would understand the term 'service' to cover advocacy performed *in coordination with, or at the direction of*, a foreign terrorist organization." *Id.* at 24 (emphasis added). The government adduced no such evidence of coordination or direction here.

The government's argument addressing "for the benefit of" is both flawed and at odds with the position it has taken in another case before this Court. In *Open Society Justice Initiative v. Trump*, the plaintiffs sought to enjoin the enforcement of IEEPA penalties for violations of executive orders and regulations enacted against persons associated with the International Criminal Court ("ICC"), which plaintiffs contended would violate, *inter alia*, their First Amendment rights to file amicus briefs in support of the ICC. 510 F. Supp. 3d 198, 202-07 (S.D.N.Y. 2001). In opposing the motion, the government stated that its position with regard to amicus briefs was that "absent facts that do not appear to apply here, such as that a brief was drafted *at the specific request of and in coordination with* [certain plaintiffs]," submitting an amicus brief "to the ICC is not prohibited." (*See* Br. in Opp. to Mot. for Preliminary Injunction, *Open Society Justice Initiative v. Trump*, No. 20 Civ. 8121, 2020 WL 10352359 (S.D.N.Y. Nov., 9, 2020) ("Gov'ts *Open Society* Br."). In addressing the informational materials exemption, the

government distinguished between materials "that are widely circulated in a standard format and those that are bespoke" and argued that the plaintiffs sought "to perform the 'bespoke' legal services of writing" amicus briefs rather than the "export" of "ready-made briefs to the Netherlands," where the ICC sits. (*Id.* at 23-24.)

Here, Mr. Storm developed and maintained software offered on a permissionless basis in a "standard format" to all users and did not provide any "bespoke" offering or services "at the specific request of" or "in coordination with" the Lazarus Group. *Cf. United States v. Atilla*, 966 F.3d 118, 128-29 (2d Cir. 2020) (evidence of sanctions evasion scheme included the goal of "convert[ing] Iranian oil proceeds" to make international payments for sanctioned Iranians, defendant's knowledge and facilitation of those payments, and communications with Iranian clients). This conclusion is further supported by the lack of evidence of any communications between Mr. Storm and the Lazarus Group, an agreement between them, or compensation paid to Mr. Storm by the Lazarus Group. *Cf. United States v. Griffith*, 515 F. Supp. 3d 106, 121 (S.D.N.Y. 2021) (government proffered "evidence that Griffith expressed a desire to return to the DPRK and help them utilize cryptocurrency"). As such, even assuming Mr. Storm's development and maintenance of the features identified by the government could be construed as a "service" (it cannot), the government adduced no evidence that Mr. Storm provided such services "to" or "for the benefit of" the Lazarus Group, mandating acquittal on Count Three.

F. The Informational Materials Exception Applies

The government disclaims the informational materials exception under the premise that it has proved a money-laundering scheme existed between Mr. Storm and the Lazarus Group. (Mot. at 92-93, 96.) But as demonstrated above, Tornado Cash is a tool, not a service. It is not subject to the IEEPA, nor has the government adduced any evidence of Mr. Storm's providing services to or for benefit of the Lazarus Group. The government's premise thus fails.

The government argues that software is not protected informational materials (Mot. at 93-94), but the exception explicitly applies to CD-ROMs, which contain software. 50 U.S.C. § 1702(b)(3).[22] The government has never explained why the exception would cover a CD-ROM but not its contents. Instead, the government argues that OFAC has exempted software from the exception under the so-called Software and Technology Regulation. (Mot. at 94). But OFAC does not have the authority to amend the IEEPA's statutory exception by regulation, nor is OFAC's interpretation of the statute entitled to deference. *See Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 413 (2024); *see also* Mot. at 95. Nor has Congress "tacitly endorsed" the government's interpretation of the regulation. (Mot. at 96 n.30.) The government's "logic" is that when Congress fixes one flawed regulation it *sub silentio* approves of all other flawed regulations it did not fix—which is absurd on its face.

Moreover, the trial evidence showed that, while the Tornado Cash protocol, like any internet-based application, itself may rely on software that facilitates data transmission, such as a web browser or file sharing service (*see* Tr. 1817:1-18), Tornado Cash is not used for "data transmission" and therefore, does not satisfy the regulation's plain language. *See* 31 C.F.R. § 510.213(c)(3). Given that nearly all software now is web-based, the government's overbroad view of "data transmission" threatens to create an all-encompassing software exception swallowing the Constitutional and statutory rules protecting informational materials. *See Fed. Election Comm'n v. Pol. Contributions Data, Inc*., 943 F.2d 190, 191 (2d Cir. 1991) ("we are obliged to construe statutes to avoid constitutional problems whenever possible").

The government argues its overbroad view should prevail because there is a lack of

[22] *See* Shapiro *et al.*, *The Invention of Compact Discs*, Dartmouth (Nov. 9, 2012), available at https://bit.ly/3K0AjMg ("Launched in 1985 … the CD-ROM stores computer software and data.").

caselaw applying the informational materials exception to software. Indeed, the government historically has not prosecuted software, presumably because of the obvious First Amendment concerns. *See Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 449-50 (2d Cir. 2001) (finding "computer code conveying information" to be protected speech"); *Bernstein v. U.S. Dep't of State*, 974 F. Supp. 1288, 1308 (N.D. Cal. 1997), *aff'd* 176 F.3 1132 (9th Cir. 1999) (encryption software regulations were unconstitutional prior restraint). No court has held that software is *not* informational materials either. The government's reliance on *Bernstein*'s *dicta* is misplaced, since the district court there found the software regulations to be unconstitutional. *Bernstein*, 974 F. Supp. at 1308.

Finally, the government lists a parade of horribles that supposedly would result should the informational materials exception thwart Mr. Storm's prosecution. (Mot. at 97-98). Oddly, the government protests that the President could not regulate banks and payment processors, even though these entities are highly regulated by Congress and the states, are subject to myriad anti-money laundering regulations, and have robust sanctions compliance regimes. Nor does the government explain why a software developer like Mr. Storm should be regulated like a bank or a payment processor, particularly where it eschewed an 18 U.S.C. § 1960(b)(1)(B) charge.

Rather than offer a legal basis for its interpretation, the government attacks the cases supporting Mr. Storm. It incorrectly distinguishes the *TikTok* cases as targeting more "expressive conduct" (Mot. at 98), but admits, as it must, that Count Three is based on the acts of hosting a website (which is code), maintaining the UI (also code), and developing the relayer algorithm (also code). At a minimum, this is indirect regulation of informational materials by using the IEEPA to reduce or eliminate use of the Tornado Cash software. *See* 50 U.S.C. § 1702(b)(3); *see also TikTok Inc. v. Trump*, 490 F. Supp. 3d 73, 81 (D.D.C. 2020); *Marland v. Trump*, 498 F.

Supp. 3d 624, 637 (E.D. Pa. 2020) (finding indirect regulation by undermining app's functionality and preventing use). That the informational materials in *TikTok* are different from those here makes no difference; if code is informational material (and it is), then the same logic applies.

Amirnazmi confirms this result. *See United States v. Amirnazmi*, 645 F.3d 564 (3d Cir. 2011). While the government argues that the software there was protected only because its "primary function was to make information … available to its users" (Mot. at 99), this "primary function" test appears nowhere in the informational materials exception or in the caselaw. Rather, as the Third Circuit explained, and as the government itself stated in *Open Society* (*see* Gov'ts *Open Society* Br.), the "key distinction" is "between informational materials . . . widely circulated in a standardized format and those that are bespoke." *Amirnazmi*, 645 F.3d at 587. As demonstrated above, the Tornado Cash software is the former, not the latter, which means it is entitled to the same protections afforded to other informational materials.

V. THIS COURT SHOULD NOT DISREGARD THE CONSTITUTIONAL IMPLICATIONS IN LIGHT OF THE EVIDENCE AT TRIAL

A. Mr. Storm Was Denied Fair Notice and Due Process, Requiring Dismissal of All Counts

The government misconstrues this Court's prior rulings on due process: the rulings were based on facial challenges. (*See* Dkt. 97 at 43 ("[Mr. Storm's] *facial* vagueness challenge, therefore, [fails].") (emphasis added).) This Court has not previously ruled on whether "the statute [was] unconstitutional *as applied*." *United States v. Milani*, 739 F. Supp. 216, 218 (S.D.N.Y. 1990) (emphasis added). Indeed, such a determination typically "await[s] conclusion of the trial." *Id.*; *see also United States v. Peraire-Bueno*, 2025 WL 2062021, at *6 (S.D.N.Y. July 23, 2025) ("While courts do occasionally find the application of a statute to particular facts unconstitutionally vague, such analysis is generally undertaken after the factual record is

developed."). As such, this Court is now free to "determine whether the [relevant] statutes failed to provide Defendant fair warning that his conduct was prohibited by law, as required by the Due Process Clause." *United States v. Phillips*, 690 F. Supp. 3d 268, 293 (S.D.N.Y. 2023).

The trial record here did not live up to the government's accusations of willful criminal conduct. Instead, the trial record amounted to *could have's* and *should have's*—a negligence theory. But criminal statutes do not impose affirmative obligations on individuals that can be retrospectively assessed for sufficiency without fair notice of such obligations, and for that reason, criminal statutes must "provide a person of ordinary intelligence fair notice of what is prohibited[.]" *United States v. Williams*, 553 U.S. 285, 304 (2008). The theoretical actions Mr. Storm could have taken, assessed by the government in hindsight, fail to give Mr. Storm *ex ante* fair notice of what was *prohibited*. As such, these statutes are unconstitutionally vague as applied to Mr. Storm and require acquittal on all counts.

Similarly, because the government has stretched these statutes beyond recognition and is seeking to impose legal duties that have no basis in statute or regulation, the rule of lenity requires their dismissal. *See Rewis v. United States*, 401 U.S. 808, 812 (1971).

B. The Tornado Cash Software Involves Expressive Conduct Protected by the First Amendment

This Court should also consider Mr. Storm's First Amendment as-applied challenge in the light of the evidence actually introduced at trial. *See Milani*, 739 F. Supp. 216, 218. The government ignores the evidence and repeats the argument in response to Mr. Storm's motion to dismiss—*i.e.*, the statutes at issue regulate function, not speech. On that basis, the government asks this Court to disregard the expressive conduct identified by Mr. Storm, (Mot. at 87-88), because it "includes the functional capability of code[.]" (Opp. at 101 (quoting Dkt. 97).)

This is not how the First Amendment works; the government cannot avoid it by arguing that software performs a function, because that is always true of software. Rather, in regulating the function of software, the government may not violate the First Amendment's protections for the expressive elements of software. *See Universal City Studios*, 273 F.3d at 451 (computer code implicates both "functional and expressive elements"; the expressive elements draw First Amendment protections).

Despite the government's claims, as applied, the statutes at issue are content-based and merit strict scrutiny. (*See* Mot. at 87-88.) At trial, the government introduced evidence, including expert testimony, focusing on the particular manner in which the Tornado Cash smart contracts and UI facilitated a user's blockchain transaction—in other words, based on the content of the code that makes up Tornado Cash—and the government then argued at closing that Mr. Storm should have written or re-written the code in other ways (*e.g.*, to include the features proposed by Mr. Werlau). The government does not even try to argue that the statutes would survive strict scrutiny; all three counts should be dismissed on First Amendment grounds. (*See* Mot. at 88-89.)

Dismissal is still appropriate even if this Court agrees that the statutes are content-neutral, because the burden on Mr. Storm's speech is more than what is necessary to further the government's interest, as it has the effect of chilling any innovation touching privacy. (Mot. at 89-90.) The government argues it "has substantial interests" in prosecuting money launderers and sanctions evaders (Opp. at 102-03), which is true but irrelevant. Mr. Storm is neither, and the undisputed evidence showed he was not the one who used Tornado Cash to launder cryptocurrency or transact with sanctioned entities like the Lazarus Group.

Finally, the statutes at issue are also facially overbroad for the same reasons already stated. (*See* Mot. at 90-91). The government responds that the statutes have a legitimate purpose

(Opp. at 104), but the fact that a statute may have "lawful applications" does not save it where, as here, the statute prohibits a substantial amount of free speech. *United States v. Hansen*, 599 U.S. 762, 769, 770 (2023).

VI. CONCLUSION

For the reasons set forth in Mr. Storm's motion and above, this Court should grant his motion for judgment of acquittal on all counts or dismiss all counts based on lack of venue.

DATED: December 12, 2025

Respectfully submitted,

By: */s/ Brian E. Klein*
Brian E. Klein
Keri Curtis Axel
Becky S. James
Kevin M. Casey
Viviana Andazola Marquez
Waymaker LLP

-and-

David E. Patton
Christopher Morel
Hecker Fink LLP

Attorneys for Roman Storm

TECHNOLOGY FACTS APPENDIX

(1) ***Tornado Cash Is Noncustodial***. Although the government takes issue with the characterization of Tornado Cash as a decentralized protocol, the undisputed facts show that Tornado Cash is noncustodial, meaning the user retained exclusive custody and control over any funds deposited into the protocol unless the user elected to share their secret note with others. (Tr. 1194:5-13 (Werlau); Tr. 1772:11-15 (Edman); 267:16-268:10 (Bram).) The secret note is similar to the private keys to a blockchain wallet address insofar as no one, not even law enforcement, can access funds held in a wallet without the private key. (Tr. 677:23-678:9 (SA DeCapua).) It is equally undisputed that Mr. Storm and the founders did not have access to the secret note or to the funds deposited into the Tornado Cash protocol. (Tr. 1147:19-20; 1198:15-1199:5 ((Werlau testifying that "only the user had access to their deposit" and agreeing that "the founders couldn't go into the pools" to access any user funds and that there was "no back door into these pools for the founders"); Tr. 1750:21-1751:1 (Edman explaining that "[n]on-custodial, as opposed to custodial, means that the developers cannot control the assets that are in the Tornado Cash protocol. So once ETH, we will say, is deposited to one of the immutable pools, the developers have no ability to unilaterally transfer those assets out of the pool or prevent the withdrawal); *cf*. Tr. 677:23-678:9 (DeCapua explaining a private key is required to "transfer the cryptocurrency from any specific address" and, without one, "you just can't get into the wallet").)

The same is true of deposits or withdrawals made through the UI; the UI did not retain the secret note. (Tr. 1147:16-20, 1152:24-1153:5 (Werlau); 1807:2-8, 1808:19-1809:6 (Edman).) The UI never took custody of any funds. (Tr. 1193:24-1194:1 (Werlau).) It is thus undisputed that, irrespective of *how* the user deposited or withdrew their funds into Tornado Cash, no one other than the user had access to or control over their funds at any point before, during, or after

the user's interaction with the protocol. And it is equally undisputed that by keeping the user in control of their funds and ensuring that this noncustodial feature could not be changed by making the pool smart contracts immutable, the protocol was safer from hacks. (Tr. 1199:13-18 (Werlau).)

(2) ***Tornado Cash Is Permissionless***. It is undisputed the Tornado Cash pools are, like most smart contracts on Ethereum, permissionless, meaning anyone with an Internet connection can access them so long as the Ethereum blockchain continues to exist. (Tr. 1161:24-1162:2 (Werlau); Tr. 1766:12-21, 1769:21-24, 1770:18-22 (Edman).) The same is true of the UI, insofar as the UI was publicly accessible to anyone in the U.S. (Tr. 1191:4-14 (Werlau); Tr. 218:1-6; 272:20-23 (Bram).) One exception applied to users who accessed the UI from the tornado.cash website after the founders implemented geo-blocking on the website in or around June 2020. (Tr. 1822:18-1823:20 (Edman).) Once the UI was hosted on IPFS, those versions of the UI were accessible to anyone. (Tr. 1823:19-20 (Edman).) Users did not have to accept the latest version of the UI uploaded to IPFS and could always access prior versions of the UI or even create their own. (Tr. 872:13-21; 876:15-877:11 (Gibbs); Tr. 1819:25-1820:2, 1926:25-1927:17 (Edman).) Another exception, discussed below, are transactions with wallet addresses sanctioned by OFAC, which were blocked on the UI through the implementation of the Chainalysis Sanctions Oracle.

(3) ***The Tornado Cash UI Blocked Transactions from Sanctioned Wallets***. The government has consistently derided Mr. Storm's implementation of the Chainalysis Sanctions Oracle onto the UI as a "half-measure" or a "fig leaf" (Opp. at 43-44, 84), but the undisputed evidence shows that the Oracle did, in fact, block OFAC-sanctioned wallets from accessing Tornado Cash via the UI. There is no dispute that Chainalysis, and not Mr. Storm, updated the Oracle to include newly sanctioned wallet addresses (Tr. 1825:17-24, 1834:23-1835:3)

(Edman)); and between the time the Oracle was implemented and August 8, 2022, there were *no deposits from any sanctioned wallet address* into the Tornado Cash smart contract pools. (Tr. 1831:14-1832:6) (Edman).) In other words, the Oracle was effective in blocking transactions from wallet addresses sanctioned by OFAC that were added to the Oracle by Chainalysis. The government's argument that the implementation was a half-measure, pointing to Mr. Storm's statements about it being "easy to bypass," is really a criticism of the Oracle itself and ignores the following related fact that is equally undisputed: there was no "full measure" available because Ethereum users could very quickly and easily generate numerous wallet addresses.

(4) *Ethereum Users Can Quickly and Easily Create New Wallet Addresses*. There is no dispute that the owner of an Ethereum wallet can quickly and easily create additional addresses. (*Id.*) There is also no dispute that, in all of the transactions identified by the government, bad actors were able to move proceeds very quickly to many different intermediary wallets before depositing into Tornado Cash. (Tr. 679:18-680:3, 680:21-681:5, 690:19-21 (DeCapua); Tr. 1760:4-5, 1762:15-1763:16 (Edman).) Thus, even where a particular wallet address is blocked because it contains funds that can be traced back to a hack, the hacker could very quickly move the funds into a different, newly created wallet to "easily" circumvent any blocking against the wallet address. (Tr. 694:15-24 (DeCapua); Tr. 1828:12-16 (Edman).) Anyone can review blockchain records to trace such transactions *after* the fact. (Tr. 483:7-16 (DeCapua); Tr. 1832: 16-23 (Edman).) But Ethereum tokens do not have any unique identifiers, so there is no way to trace the flow of particular tokens in an automated matter. (Tr. 1833:3-5 (Edman).) The government cannot dispute that no company or government organization offered any technical solution to trace such transactions in real-time. (Tr. 1833:6-11 (Edman).)

(5) ***Relayers Were Third Parties***. It is undisputed that the relayers were third parties. (*See* Tr. 1048:8 (Werlau: "relayer[] network was a collection of third-parties[.]"); Tr. 1072:16-18 (Werlau: "relayer network was a network of third parties [who] would execute a withdrawal on behalf of users."). Also undisputed is that relayers set and collected their own fees, which were not shared with the founders. (Tr. 1073:10-12 (Werlau: "relayers would execute the withdrawal, and . . . keep a portion of the withdrawal funds to compensate them for their service as well as compensate them for the gas that this paid."); Tr. 1213:13-16 (Werlau (same)); Tr. 1779:22-24 (Edman).) Ahmed, the government's witness who used Tornado Cash, described a relayer as "a third-party entity that will perform the withdrawal on your behalf[.]" (Tr. 899:25-890:1.)

(6) ***The UI Did Not Write Transactions to the Blockchain***. The government concedes that the UI did not write *deposit* transactions to the blockchain. (*See* Opp. at 65.) The UI communicated with the software for the user's wallet, where the digital assets were stored, and it was indisputably the user's wallet software that effectuated the transfer on the blockchain. (Tr. 952:17-21 (Dubash: "Q. For example, if a user has a MetaMask wallet and they want to make a transfer of funds using that wallet, ultimately it is the wallet that would connect and send the write request to the blockchain; is that correct? A. Correct.").) It is also undisputed that the UI did not write withdrawal transactions. (Tr. 1154:7-1155:17 (Werlau explaining UI sends a withdrawal request to a relayer "over traditional web connections," and the relayer then "actually moves that information onto the blockchain").)

(7) ***Mr. Werlau's User Registry Proposal Would Require (1) the Collection of Personal Identifying Information and (2) the Maintenance of an Off-Chain Database Connecting Deposits and Withdrawals, Destroying Privacy***. Mr. Werlau described his proposal as having two components: (1) an on-chain user registry that maintains a database of user accounts and

associated wallets; and (2) an off-chain database that records all withdrawal addresses associated with a specific user account. (Tr. 1157:14-1158:17). As to the first component, it was left unclear what personal identifying information would be collected in addition to the creation of a username and password—Mr. Werlau testified only that the founders "could also collect other information if they chose, such as IP address," but did not specify what types of information. (Tr. 1160:18-21; *see also* Tr. 1222:25-1223:4 ("User name and password at minimum.").)

To the extent Mr. Werlau was suggesting the founders should collect the sort of personal identifying information required by centralized exchanges, his proposal would have effectively required the founders to implement full KYC and AML measures, which were the subject of extensive pretrial discussions. (See 7/8/2025 Tr. 57:22-6-65:12.) This Court noted that, to the extent the government elicited testimony regarding KYC or AML, the defense would be entitled to call an expert to address "the BSA regulatory structure and how the terms that the government is using pertain to a different system that's not being charged here." (Id. 59:23-60:3.) Perhaps with that admonition in mind, Mr. Werlau did not specify the types of information that would be collected.

As to the second component, Mr. Werlau's proposed the creation of "an off-chain database maintaining the connection between deposits and withdrawals." (Tr. 1157). In other words, the founders would have been required to manually maintain a database matching up a user's deposits to their withdrawals, destroying the privacy feature that was the very point of Tornado Cash. (Tr. 1188:12-14 ("In my proposal, the owners of Tornado Cash, while also maintaining a database of this transaction information, would be responsible for maintaining updates to the user registry.").) That is a far cry from the obvious fix that "any idiot would have

known to have put in place that [Mr. Storm] knew about and elected not to put in place," which was what the government represented would be Mr. Werlau's testimony. (*See* Tr. 62:2-10.)

Mr. Werlau's user registry was unlike the relayer registry. The relayer registry could be implemented by smart contract and ran autonomously, as it simply checked blockchain data to confirm that the proposed relayer had registered its wallet address and still had the requisite amount of TORN staked. (Tr. 1155:3-11.) Relayers added themselves to the registry by staking TORN; they were not required to submit their names or any other information, and their inclusion in the registry did not require verification or approval by anyone, including the founders. (Tr. 1839:12-1840:1 (Edman).) In simple terms, the relayer registry was a smart contract that confirmed whether a particular wallet address has staked sufficient TORN. By contrast, Mr. Werlau's proposal involved multiple registries, one of which would be maintained off-chain and updated manually by the founders, with no explanation as to how the founders could have feasibly implemented this feature given the volume of users and transactions.