UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

v.

ROMAN STORM and
ROMAN SEMENOV,

Defendants.

**SEALED INDICTMENT**

23 Cr.

23 CRIM 430

## OVERVIEW

1. From at least in or about 2019, up to and including at least on or about August 8, 2022, ROMAN STORM and ROMAN SEMENOV, the defendants, developed, marketed, and operated a cryptocurrency mixing service known as Tornado Cash, a business from which they sought to make, and did make, substantial profits. The Tornado Cash service combined multiple unique features to execute anonymous financial transactions in various cryptocurrencies for its customers. Claiming to offer the Tornado Cash service as a "privacy" service, the defendants in fact knew that it was a haven for criminals to engage in large-scale money laundering and sanctions evasion. Indeed, as the defendants well knew, a substantial portion of the funds the Tornado Cash service processed were criminal proceeds passed through the Tornado Cash service for purposes of concealment. The defendants also knew that the Tornado Cash service received funds from, and provided services to, the Lazarus Group, a U.S.-sanctioned North Korean cybercrime organization, by receiving, transferring, and dealing in cryptocurrency from an Ethereum wallet that was publicly attributed to the Lazarus Group and designated as blocked property.

2. At all times relevant to this Indictment, ROMAN STORM, the defendant, was a naturalized United States citizen who resided in the United States. In an interview video recorded on or about October 4, 2021, STORM described himself as the "cofounder of [the] Tornado Cash

protocol." Along with ROMAN SEMENOV, the defendant, and another person ("CC-1"), STORM was one of three principal cofounders who developed and operated the Tornado Cash service from its initial public launch in 2019 up to and including at least on or about August 8, 2022, when the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC") announced the imposition of sanctions on Tornado Cash.

3. ROMAN SEMENOV, the defendant, is a Russian citizen. In a public posting to a social media service on or about March 20, 2022, SEMENOV shared a link to an article containing an interview with himself, in which he was described as "one of the founders of Tornado Cash." Along with ROMAN STORM, the defendant, and CC-1, SEMENOV was one of three principal cofounders who developed and operated the Tornado Cash service from its initial public launch in 2019 up to and including at least on or about August 8, 2022.

**The Ethereum Blockchain**

4. Ether ("ETH") is a decentralized form of electronic currency, or cryptocurrency, existing entirely on the Internet and not in any physical form. The currency is not issued by any government, bank, or company, but rather is generated and controlled automatically through computer software operating on a "peer to peer" network. ETH transactions are processed collectively by the computers composing the network, which are referred to as "nodes."

5. To acquire ETH in the first instance, a user typically purchases it from an ETH "exchanger." In return for a commission, ETH exchangers accept payments of currency in some conventional form (cash, wire transfer, or otherwise), or payments of another type of cryptocurrency, and exchange the money for a corresponding number of ETH, based on a fluctuating exchange rate. Exchangers also accept payments of ETH and exchange the ETH back for conventional currency or another type of cryptocurrency, again charging a commission for the

service.

6. Once a user acquires ETH, the ETH is stored as a balance in an Ethereum "address," designated by a string of letters and numbers. The user can manage the Ethereum address with software or hardware known as an Ethereum "wallet," which is controlled by a "private key" known to the wallet's owner. The Ethereum address is analogous to the account number for a bank account, while the wallet is analogous to a portfolio of bank accounts, since a single wallet can contain multiple Ethereum addresses. A private key is akin to a PIN or password that allows a user the ability to access and transfer value associated with the Ethereum address. Once an Ethereum user funds an address in his or her wallet with ETH, the user can then use the ETH to conduct financial transactions, by transferring ETH to the Ethereum address of another user. This is accomplished over the Internet, by sending a message announcing the transfer to the Ethereum peer-to-peer network.

7. All ETH transactions are recorded on a public ledger known as the "Ethereum blockchain," which is stored on the nodes that make up the Ethereum peer-to-peer network. The Ethereum blockchain records the balance held in each Ethereum address and records all ETH transactions between Ethereum addresses. This public ledger serves to prevent any user from spending more ETH than the user holds in his or her Ethereum address. The public nature of the Ethereum blockchain also means that the movement of funds over the Ethereum blockchain can be traced. However, the Ethereum blockchain only reflects the movement of funds between anonymous Ethereum addresses and therefore cannot by itself be used to determine the identities of the persons involved in the transactions.

8. The Ethereum blockchain also stores computer programs known as "smart contracts." A smart contract is a computer application hosted on the Ethereum blockchain that can

hold ETH in an Ethereum address and release it when the smart contract receives instructions that comply with the smart contract's code. The Ethereum blockchain stores all transactions and balances associated with smart contracts.

**Background on the Tornado Cash Service**

9. ROMAN STORM and ROMAN SEMENOV, the defendants, working primarily with CC-1 (collectively, the "Tornado Cash founders"), began developing the Tornado Cash service in or around 2019. They launched the service in or about August 2019, when they released a public statement on the Internet with a link to the Tornado Cash website, where the Tornado Cash user interface and other materials relating to the Tornado Cash service were accessible. The announcement referred to the Tornado Cash service as a "mixer" and advertised that it "allows you to send Ethereum cryptocurrency 100% anonymously using groundbreaking, non-custodial technology based on strong cryptography!"

10. In various public and private statements from 2019 through at least on or about August 8, 2022, the Tornado Cash founders described and marketed the Tornado Cash service as allowing its customers to conduct anonymous and virtually untraceable financial transactions on the Ethereum blockchain. The Tornado Cash service provided a seamless and fully integrated service that executed anonymous transactions in ETH and certain other cryptocurrencies for its customers (the "Tornado Cash service"). Customers of the Tornado Cash service could make deposits of ETH into the Tornado Cash service and then withdraw ETH from the Tornado Cash service to a new Ethereum address, without any connection between the deposit and withdrawal on the public Ethereum blockchain. The Tornado Cash founders created and promoted the Tornado Cash service's principal operating features. This included a website and a user interface (the "UI") that interacted with various smart contracts hosted on the Ethereum blockchain, including multiple

smart contracts that held large volumes of commingled customer deposits (the "Tornado Cash pools"). The Tornado Cash service also included a network of "relayers" who provided customers with enhanced anonymity in exchange for a fee. The Tornado Cash service operated principally on the Ethereum blockchain and processed transactions primarily in ETH. However, the Tornado Cash service also provided services for certain other cryptocurrencies that use the Ethereum blockchain and for certain cryptocurrencies that use other blockchains.

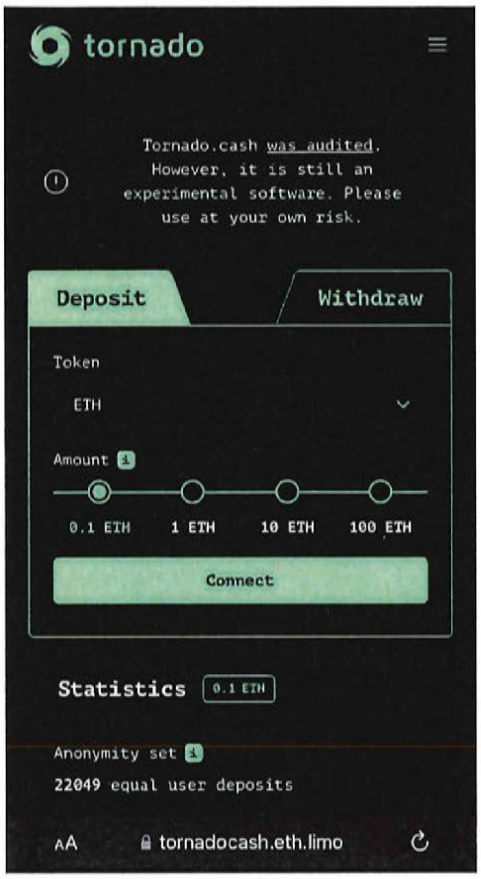
11. In 2019 and 2020, the Tornado Cash founders approached various investors to obtain financing for the Tornado Cash service. In a presentation to potential investors that he prepared in or around January 2020, ROMAN STORM, the defendant, explained that the Tornado Cash service "improves transaction privacy by breaking the on-chain link between recipient and destination addresses. It uses a smart contract that accepts ETH deposits that can be withdrawn by a different address. Whenever ETH is withdrawn by the new address, there is no way to link the withdrawal to the deposit, **ensuring complete privacy**" (emphasis in original).

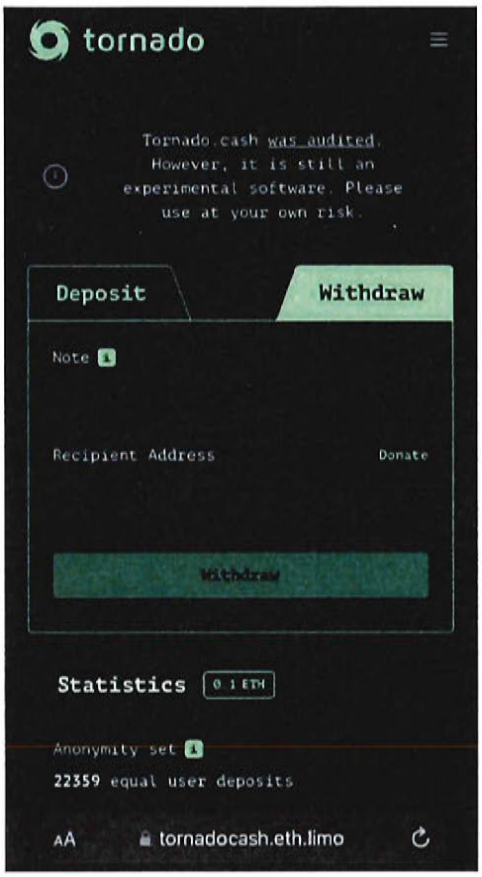
12. The Tornado Cash founders eventually obtained financing from a California-based venture capital fund ("Venture Capital Fund-1"), among other investors. On or about August 24, 2020, Venture Capital Fund-1 transferred approximately $900,000 to a bank account in the name of a company owned and controlled by the Tornado Cash founders, Peppersec Inc., that was held at a bank located in New York, New York (the "Peppersec Bank Account"). The purpose of this transfer was to finance the Tornado Cash service's startup and operations costs in exchange for an expectation that Venture Capital Fund-1 would receive a share of future profits from the Tornado Cash service.

13. At all times relevant to this Indictment, customers of the Tornado Cash service, including customers based in the United States and in the Southern District of New York in

particular, were able to and did in fact deposit funds into the Tornado Cash service in one of two ways: (i) through the UI, a computer application designed by the Tornado Cash founders and accessible through any standard internet browser; or (ii) by sending funds to the Tornado Cash pools by interacting with the smart contracts directly, thereby bypassing the UI. This latter option required a degree of technical sophistication that the UI did not require.

14. At all relevant times, ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 exercised control over the Tornado Cash UI. The Tornado Cash founders used the Peppersec Bank Account to pay for a web hosting service located in the United States to host the Tornado Cash website. The website provided access to the UI, which the founders posted to a decentralized network that was accessible through a United States-hosted web gateway. These steps ensured that the UI was accessible to customers of the Tornado Cash service using any standard internet browser. The Tornado Cash founders had the ability to make changes to the UI at their own discretion. Screenshots taken from the UI during the relevant time period are below:




15. As shown in the screenshots of the UI above (the "UI Screenshots"), a customer of the Tornado Cash service could connect the customer's Ethereum wallet to the UI, and the customer could then simply go to the "Deposit" tab, select the amount of ETH to be deposited from one of four choices (0.1 ETH, 1 ETH, 10 ETH, or 100 ETH), and then connect to execute the transaction. The UI would execute the transaction by initiating a transfer of the selected amount from the customer's Ethereum address to one of the Tornado Cash pools. The UI also would provide a unique "secret note" to the Tornado Cash customer for each deposit, and the customer would be the only person with access to the secret note.

16. To make a withdrawal from the Tornado Cash service, the customer would go to the "Withdraw" tab on the UI and enter the secret note that the customer had received when making the deposit, along with the recipient address where the withdrawal should be transmitted. The

Tornado Cash UI would then initiate a transfer of the amount correlating with that secret note from the Tornado Cash pools to the customer-designated recipient address.

17. The Tornado Cash service used multiple methods to obfuscate the link between its customers' deposits and withdrawals, and marketed its ability to do so. For example, the Tornado Cash service mixed together multiple customer ETH deposits into the Tornado Cash pools, which were governed by smart contracts developed by the Tornado Cash founders. When a customer deposited ETH into the Tornado Cash service, that ETH was sent to one of the Tornado Cash pools and commingled with other customer deposits. The Tornado Cash founders released the first Tornado Cash pool on the Ethereum blockchain in or about August 2019, and developed and released additional Tornado Cash pools over time.

18. When a customer deposit of ETH was transferred into a Tornado Cash pool, the ETH was added to the preexisting ETH held in that Tornado Cash pool. That is, the deposit became commingled and indistinguishable from other deposits. When a customer later submitted a secret note to the Tornado Cash UI for the purpose of making a withdrawal to an Ethereum blockchain address designated by the customer, the UI sent the secret note to a smart contract created by the Tornado Cash founders to initiate a withdrawal from the corresponding Tornado Cash pool. The smart contract validated the secret note, and then the corresponding amount of ETH was transferred from the Tornado Cash pool to the customer-designated address. The ETH used for the withdrawal was taken from the total balance of commingled deposits held in the pool. There was no public link between the particular ETH that were deposited into the Tornado Cash service and the particular ETH that were withdrawn. As a result, while all deposits into and withdrawals from the Tornado Cash service were visible on the Ethereum blockchain, that blockchain did not show which deposits corresponded with which withdrawals.

19. The Tornado Cash service further severed the link between sender and recipient by only permitting deposits in 0.1, 1, 10, and 100 ETH increments, and featured individual Tornado Cash pools for each ETH increment. If, for example, a customer of the Tornado Cash service wanted to send 37 ETH to someone, the service would not permit a single 37 ETH deposit into a single pool, but rather multiple deposits which were sent to multiple pools that would add up to 37 ETH (e.g., three 10 ETH deposits to the 10 ETH pool and seven 1 ETH deposits to the 1 ETH pool, or another combination of deposits chosen by the customer). For each of these deposits, the UI would provide a unique secret note that could be used to make a withdrawal. This feature of the Tornado Cash service purposefully made it difficult, if not impossible, for someone to attribute any withdrawal or set of withdrawals to a particular deposit or set of deposits through analysis of the public blockchain. The public Ethereum blockchain transactions for each of the Tornado Cash pools would show nothing but a uniform stream of deposits and withdrawals of the same amount of ETH.

20. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 also encouraged customers of the Tornado Cash service to wait a period of time (for example, several days) after depositing funds before making withdrawals, in order to further disguise the link between any deposit and withdrawal. It was assumed that during this period of delay the Tornado Cash service would have other deposits and withdrawals, thus further obscuring the link between any particular deposits and withdrawals. For this reason, STORM, SEMENOV, and CC-1 encouraged customers to leave their funds in the Tornado Cash pools for as long as possible to increase their anonymity. For instance, in a video recorded media interview on or about October 4, 2021, STORM stated that "it's good for anyone to wait sometimes, wait for more, let's say, participants to join the pool, and then you can withdraw later on when you feel you have a

sufficient privacy."

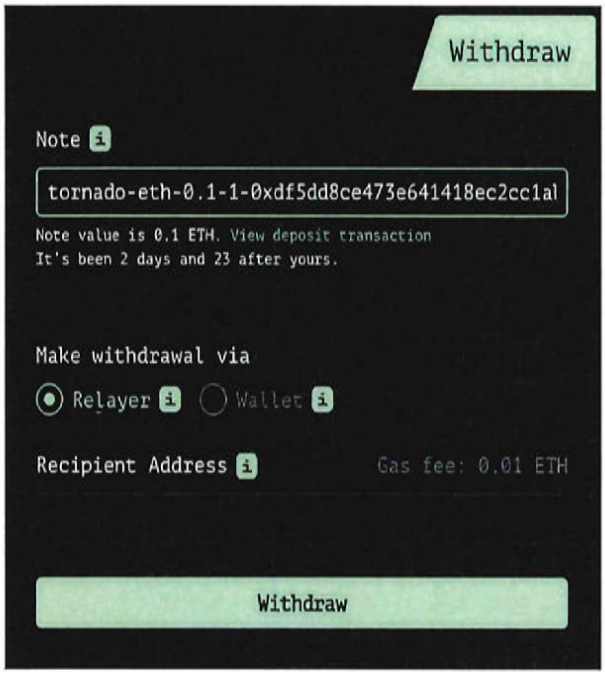
21. As noted above, directly accessing the smart contracts for the Tornado Cash pools that the Tornado Cash founders created required technical sophistication. The Tornado Cash UI, however, functioned as a user-friendly interface that attracted a large customer base and was a key component of the Tornado Cash service. The anonymity value of the Tornado Cash service increases with the size of its customer base. In the October 4, 2021 interview, ROMAN STORM, the defendant, explained that "the less people use the pool, the less privacy you have, and the more people use the pool, the better your privacy." Because of this, the larger pools of deposits that were made possible by the UI were valuable even to sophisticated customers who could interface directly with the smart contracts, because those customers' deposits were mixed with all the other deposits that were made by customers through the UI.

22. To assist customers of the Tornado Cash service in increasing the anonymity of their transactions, ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 designed the UI to display the so-called "anonymity set" for a particular Tornado Cash pool. For example, at the time the UI Screenshot on the left above was taken, the anonymity set for the 0.1 ETH pool was approximately 22,049 "equal user deposits." In other words, the UI published statistics about the approximate number of deposits in each pool in order to assure customers that their deposits would indeed be sufficiently obscured by the presence of many other deposits, as relatively few deposits within a pool would make withdrawals from that pool theoretically easier to trace.

23. The Tornado Cash UI required an interface to connect to and communicate with the smart contracts on the Ethereum blockchain to execute transactions. Due to the large volume of transactions in which the Tornado Cash service engaged, the Tornado Cash founders contracted

with a service provider located in the United States that facilitated large volumes of traffic flowing between the UI and the Ethereum blockchain. ROMAN STORM, the defendant, made regular payments to this service provider in 2021 and 2022, using a debit card in his name that was connected to the Peppersec Bank Account.

24. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 designed and promoted the use of "relayers" as an additional feature of the Tornado Cash service that provided enhanced anonymity to its customers. Without a relayer, a customer of the Tornado Cash service seeking to withdraw ETH needed to use a wallet that already contained a balance of ETH to make the withdrawal, because the Ethereum network charges a fee in ETH for each transaction, which is referred to as the "gas" fee. However, the Tornado Cash service allowed its customers to choose to have a Tornado Cash relayer transmit the secret note to the Tornado Cash smart contract, with the relayer paying the attendant gas fee to the Ethereum network; the relayer would pay to host a "relayer node" that would transmit the secret note and gas fee. In turn, the relayer could deduct a fee from the customer's withdrawal amount to pay for the gas fee, and could deduct an additional fee as payment for the relayer's services. The relayers therefore provided customers of the Tornado Cash service with enhanced anonymity in exchange for a fee charged per transaction, because they allowed customers to make withdrawals to a new Ethereum address with no prior transaction history. The option to withdraw using a relayer was included on the Tornado Cash UI, as shown in the following screenshot:




25. Without relayers, the gas fee requirement to execute transactions would have prevented customers of the Tornado Cash service from creating new and completely anonymous—and thus untraceable—wallets to receive their withdrawals from the Tornado Cash service. The customer would have had to make a transfer of the gas fee to such a wallet to pay for the withdrawal. That transfer of the gas fee would have been traceable on the Ethereum blockchain, and thus could have potentially compromised the anonymity of the person making the withdrawal. Several U.S. persons acted as relayers for the Tornado Cash service, and paid for services located in the United States to host their relayer nodes.

26. Initially, beginning in or about August 2019, ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and CC-1 exercised complete control over the Tornado Cash service. In or about May 2020, the Tornado Cash founders announced that the smart contracts for the Tornado Cash pools had been updated to remove the founders' private keys, meaning that no one could further modify those smart contracts. In or about December 2020, the Tornado Cash founders created a decentralized autonomous organization (the "Tornado Cash DAO") to make

certain governance decisions regarding the Tornado Cash service, with the founders retaining control over other decisions such as the operation and design of the UI.

27. In connection with the creation of the Tornado Cash DAO, the Tornado Cash founders made a public announcement of the creation of a new token on the Ethereum blockchain, called the TORN token, and created approximately 10 million TORN tokens. Pursuant to a formula created by ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1, approximately 30% of the TORN tokens were distributed to the three founders and to certain investors in the Tornado Cash service, including Venture Capital Fund-1. STORM, SEMENOV, and CC-1 each received approximately 8% of the total number of TORN tokens, or approximately 800,000 TORN tokens each. The remaining TORN tokens were distributed in three ways: some were distributed to early users of the Tornado Cash service; some were distributed to an "Anonymity Mining" fund that would be used to incentivize customers to deposit ETH into the Tornado Cash pools for extended periods of time to enhance the anonymity of the pools; and some were distributed to a "DAO Treasury" that would be controlled by the Tornado Cash DAO. After an initial period in which TORN tokens were locked, they were unlocked and could be freely traded, which gave holders of TORN tokens an incentive to increase the value of TORN tokens.

28. The Tornado Cash DAO was set up to make certain governance decisions for the Tornado Cash service. Anyone who owned TORN tokens could participate in the DAO by depositing, or "staking," the TORN tokens into a smart contract referred to as the "governance contract." The Tornado Cash founders and others could propose changes to the Tornado Cash service, which could be voted on by anyone who had staked TORN tokens in the governance contract.

29. After the creation of the TORN tokens, ROMAN STORM and ROMAN

SEMENOV, the defendants, and CC-1 and others, devised and implemented a plan to profit from the fees charged by relayers to customers of the Tornado Cash service. In or about February 2022, the Tornado Cash founders, working with others, released a plan to incorporate an algorithm into the Tornado Cash UI that would select a relayer for each withdrawal. The Tornado Cash DAO voted in favor of this plan, which was put into effect on or about March 2, 2022.

30. The relayer algorithm selected relayers only from those who had staked at least 300 TORN tokens into a new smart contract, which would place that relayer on a list maintained in a smart contract referred to as the "Relayer Registry." When a customer of the Tornado Cash service initiated a withdrawal through the UI, the UI's algorithm would retrieve the list of relayers from the Relayer Registry and select a relayer using a mathematical formula that took into account how many TORN tokens each relayer had deposited and the fee being charged by each relayer. The more TORN tokens that a relayer deposited into the Relayer Registry smart contract, the higher that relayer's chance of being selected for a withdrawal. This algorithm served to boost the value of TORN tokens because it gave Tornado Cash relayers an incentive to purchase and stake more TORN tokens.

31. Additionally, whenever a relayer was selected by the Tornado Cash UI, some of the TORN tokens staked by that relayer would be transferred to another smart contract, where they would be distributed to the holders of TORN tokens who had a stake in the Tornado Cash governance smart contract. This required relayers to continually replenish their TORN tokens to maintain their chances of being selected by the Tornado Cash UI to process withdrawals, thus creating steady demand for TORN tokens and upward momentum for their value. In substance, by distributing the relayers' TORN tokens to the holders of TORN who participated in the Tornado Cash DAO, the relayer algorithm allowed the holders of TORN tokens to profit by obtaining a

share of the profits generated by relayers from charging fees for Tornado Cash withdrawals.

**The Operation of the Tornado Cash Service Without Know Your Customer or Anti-Money Laundering Programs**

32. Under federal law, all money transmitting businesses, including businesses engaged in transmission of cryptocurrencies such as ETH, are required to register with the United States Department of the Treasury's Financial Crimes Enforcement Network ("FinCEN"). Money transmitting businesses are also required to comply with certain aspects of the Bank Secrecy Act, such as filing reports of suspicious transactions, *see* 31 U.S.C. § 5318(g); 31 C.F.R. § 1022.320(a); and implementing an effective anti-money-laundering ("AML") program, *see* 31 C.F.R. § 1022.210. An effective AML program is described as "one that is reasonably designed to prevent the money services business from being used to facilitate money laundering and the financing of terrorist activities." 31 C.F.R. § 1022.210(a). Under the regulations, an AML program must, at a minimum, "[i]ncorporate policies, procedures, and internal controls reasonably designed to assure compliance" with a money service business's obligations to verify customer identification, file reports, create and retain records, and respond to law enforcement requests. 31 C.F.R. § 1022.210(d)(1). The obligation to verify customer identification is frequently referred to as a "know your customer," or "KYC," requirement.

33. Throughout the time period charged in this Indictment, ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1, together with others involved in the Tornado Cash service, including the relayers, engaged in the business of transferring funds on behalf of the public. However, neither the Tornado Cash service, nor any of the Tornado Cash founders, was registered with FinCEN as a money transmitting business.

34. Throughout the time period charged in this Indictment, the Tornado Cash service failed to establish an effective AML program or to engage in any KYC efforts. Customers of the

Tornado Cash service could access the Tornado Cash UI to make deposits to and withdrawals from the Tornado Cash service without providing any identifying information aside from an address on the Ethereum blockchain. As discussed below, this failure to implement AML/KYC facilitated the ability of customers of the Tornado Cash service to transfer criminal proceeds between addresses on the Ethereum blockchain without being traced, and to engage in transactions meant to conceal the nature, location, source, ownership, and control of criminal proceeds.

35. Indeed, as stated above, ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 specifically promoted the Tornado Cash service for its ability to provide customers with anonymous transactions. For instance, the Tornado Cash founders created and paid for a public repository of documents and computer code on an internet hosting service, which ROMAN STORM, the defendant, paid for with his debit card connected to the Peppersec Bank Account. This website contained computer code relating to the Tornado Cash service, as well as documents with information and guidance on how to use the Tornado Cash service. One of these documents, titled "Tips to Remain Anonymous," included the following description: "The Tornado Cash tool allows you to remain anonymous on chain." This document then provided a number of "tips" for customers, including that customers should "consider using TOR and/or a VPN for your transfers," that they should "delete data" from their web browsers "after each deposit or withdrawal," and that they should "be patient" about making withdrawals, because "the longer you wait, the greater your anonymity will be." TOR is an internet browser that routes internet traffic through a series of different routers to conceal the IP address of the person using it. A VPN, or virtual private network, is a service that routes a user's internet traffic through a separate server, which makes it appear to other devices on the internet that the user is accessing the internet from a different IP address than the user is actually using.

36. Similarly, the Tornado Cash UI, which ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 developed and operated, advised customers of the Tornado Cash service on how to ensure further anonymity. The UI advised customers to "make sure to use different IP addresses for deposit and withdrawal (and further operations with withdrawal account). We recommend using TOR browser or VPN service." On or about September 26, 2019, STORM wrote a public Tweet highlighting this language from the UI.

37. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 knew full well that they could have implemented AML and KYC programs in the Tornado Cash service, but determined not to do so. For instance, on or about November 16, 2021, STORM sent SEMENOV and CC-1 a message using an encrypted messaging application (the "Encrypted App") with a link to a website that contained instructions for installing an AML program with KYC features into an Ethereum-related application. In response, on the same date, SEMENOV asked "Would you like to install KYC on tornado?" STORM responded on the following date, writing "I'm fucking speechless / after such suggestions."[1] After exchanging these messages, STORM and SEMENOV took no steps to install KYC or implement an AML program in the Tornado Cash service.

38. In or about May 2022, ROMAN STORM, the defendant, sent a message to ROMAN SEMENOV, the defendant, CC-1, and representatives of Venture Capital Fund-1 through the Encrypted App, discussing the possibility of a service that offered "privacy for blockchain with full compliance … basically fork of tornado cash but with KYC/AML in it." The investors at Venture Capital Fund-1 dismissed the idea, with one of them writing "I just don't know if anyone will actually want this. Market need seems quite thin." The investor went on to

[1] This and many of the other Encrypted App messages quoted in this Indictment were originally written in Russian. For messages that were originally written in Russian, the quoted language has been translated from the original Russian by an interpreter.

say that "it would be unlikely that as a fund we'd use a 'compliant mixer.'" STORM, SEMENOV, and CC-1 took no further steps to integrate KYC, AML, or any other form of "full compliance" into the Tornado Cash service.

39. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 did include on the Tornado Cash UI an optional feature referred to as the "compliance tool." The compliance tool allowed a customer of the Tornado Cash service to generate a report using a secret note to identify which deposit and which withdrawal corresponded to that secret note. This enabled customers of the Tornado Cash service to document their own transaction history if they chose to do so. However, the Tornado Cash service's "compliance tool" did not require customers to provide the Tornado Cash service with any identifying information, and did not enable the Tornado Cash service to engage in any transaction monitoring, recordkeeping, reporting, or other AML compliance measures. The "compliance tool" was also entirely optional for customers of the Tornado Cash service, and ROMAN STORM, the defendant, described it in a video recorded interview as being an "opt-in feature."

40. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 recognized that they did not incorporate KYC or AML programs as required by law, and so they made misleading public statements to minimize their ownership and control of the Tornado Cash service, and their operation of the Tornado Cash service as a business from which they expected to generate substantial profits. On or about October 26, 2021, STORM sent a message to SEMENOV and CC-1 through the Encrypted App attaching a link to a Tweet discussing U.S. regulation of cryptocurrency businesses, and then sent a message in which he stated that "we should never, even in private chats, talk as if we own tornado."

41. For instance, on or about October 4, 2021, ROMAN STORM, the defendant,

participated in a video recorded interview in which he misleadingly stated that the Tornado Cash service was "not for profit. It's not a commercial project." In fact, as STORM well knew, he and the other Tornado Cash founders had developed the Tornado Cash service as a business, had pitched it to investors as an opportunity to make profits, and were in fact operating the Tornado Cash service with the intention of making profits from increasing the value of their TORN tokens.

42. On or about March 20, 2022, ROMAN SEMENOV, the defendant, issued a public Tweet in which he misleadingly stated, in part, that "my opinion cannot affect [the Tornado Cash service] even if I really wanted to change something." In fact, as SEMENOV well knew, he and the other Tornado Cash founders had control over multiple features of the Tornado Cash service, including the Tornado Cash UI. SEMENOV and the other Tornado Cash founders had the ability to implement a KYC process, an AML program, and other compliance features into the Tornado Cash UI, but had chosen not to do so.

43. On or about March 15, 2022, ROMAN SEMENOV, the defendant, sent a message to ROMAN STORM, the defendant, and CC-1 through the Encrypted App, in which SEMENOV pasted the text of an article about the United Kingdom's National Crime Agency calling for stricter regulation of decentralized cryptocurrency mixing services. On the same date, STORM responded that the article left him "full of anxiety," noting "for now it's just btc mixers but soon they'll get to tornado and start fucking our brains." SEMENOV responded that "we need to think what else they can accuse us of." STORM responded by saying: "UI + that we don't fucking block anything in the front," and then wrote that "we need to hand over the primary access and then we can yell that the Worker is not the owner."

44. Nonetheless, ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and CC-1 continued to exercise control over the Tornado Cash UI and to pay to

maintain critical infrastructure for the Tornado Cash service, and took no steps to block or even monitor deposits or withdrawals, or to collect any identifying information from customers of the Tornado Cash service. On or about May 5, 2022, CC-1 sent a message to STORM and SEMENOV through the Encrypted App, asking "I just wondered from a legal point of view, is everything ok here? Maybe it's a dead giveaway if we pay for tornado from the peppersec account."

**The Tornado Cash Service Was a Vehicle for Money Laundering**

45. The Tornado Cash founders' failure to establish an effective AML or KYC program for the Tornado Cash service facilitated its use by criminal actors laundering high volumes of criminal proceeds. Because the Tornado Cash service provided its customers with a method to engage in transactions and move funds on the Ethereum blockchain in ways that could not be traced on the public blockchain, not all of the funds passing through the Tornado Cash service can be attributed to particular actors. However, at a minimum, at least over $1 billion in criminal proceeds were laundered through the Tornado Cash service between its launch and August 8, 2022.

46. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 were aware at least as early as September 2020 that the Tornado Cash service was being used in connection with specific cyber crimes. Between in or about September 2020 and in or about August 2022, STORM, SEMENOV, and CC-1 regularly received and reviewed complaints via emails, text messages, and posts on internet forums for customers of the Tornado Cash service, in which victims of hacking, fraud, and other crimes alerted the Tornado Cash founders that the proceeds of such crimes had been deposited into the Tornado Cash service. The Tornado Cash founders also regularly exchanged messages with each other about public reporting on specific cyber crimes that were using the Tornado Cash service to launder criminal proceeds. The crimes described to the Tornado Cash founders in the complaints from victims, and described in the public reporting that

was reviewed and discussed by the Tornado Cash founders, included crimes involving computer fraud and abuse, in violation of Title 18, United States Code, Section 1030, and crimes involving wire fraud, in violation of Title 18, United States Code, Section 1343.

47. For instance, in or about September 2020, a cryptocurrency exchange ("Cryptocurrency Exchange-1") suffered a hacking incident that was widely reported on in the media. Millions of dollars in proceeds from this hacking incident were deposited into the Tornado Cash service. On or about October 25, 2020, an employee of Cryptocurrency Exchange-1 sent an email to an email address used by all three Tornado Cash founders. In this email, the Cryptocurrency Exchange-1 employee informed the Tornado Cash founders that "the hacker of [Cryptocurrency Exchange-1] has transferred the ETH to your platform," and requested assistance in blocking or tracing the funds. ROMAN STORM, the defendant, responded to the email, declining to offer any assistance.

48. In or about December 2021, another cryptocurrency exchange ("Cryptocurrency Exchange-2"), publicly announced that it had suffered a security breach caused by a stolen private key, resulting in the theft of approximately $200 million worth of cryptocurrency. Millions of dollars in proceeds from this security breach were deposited into the Tornado Cash service. On or about December 14, 2021, an attorney for Cryptocurrency Exchange-2 sent a letter to the Tornado Cash founders, stating, in sum and substance, that Cryptocurrency Exchange-2 had traced the proceeds of the security breach to the Tornado Cash service, and informing the Tornado Cash founders that "it appears that Tornado Cash is in possession of stolen Assets." ROMAN SEMENOV, the defendant, responded to the attorney, declining to offer any assistance.

49. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 were also aware that there was a widespread public perception that one of the primary uses of the Tornado

Cash service was for money laundering, and they knew that this perception was consistent with the large volume of money laundering transactions that the Tornado Cash service was in fact processing. For example, on or about November 18, 2021, STORM, SEMENOV, and CC-1 exchanged messages through the Encrypted App about a software developer they had hired who was quitting his job with the Tornado Cash service. In these messages, SEMENOV stated that "I got it, his relatives think that tornado is about money laundering and hacking." STORM responded by sending a link to a news article about how three employees of a cryptocurrency-based Internet marketplace had been indicted in the Southern District of New York for money laundering and other crimes.

50. Despite knowing full well that the Tornado Cash service was being used to launder criminal proceeds, and that the Tornado Cash pools contained large amounts of ETH representing criminal proceeds that were commingled with other customer deposits for the purpose of concealment, the Tornado Cash founders took no steps to implement effective AML or KYC programs. On the contrary, the founders took steps to increase the anonymity features of the Tornado Cash service, and to increase the degree to which they could profit from the large volume of money laundering transactions they were facilitating and participating in through their operation of the Tornado Cash service. For instance, on or about March 2, 2022, the Tornado Cash founders implemented the relayer algorithm. This increased the anonymity-enhancing effects of the relayer network by making it easier for more relayers to join the network through purchasing TORN tokens.

**The International Emergency Economic Powers Act and the Relevant Executive Orders and Regulations Regarding Sanctions**

51. The International Emergency Economic Powers Act ("IEEPA"), codified at Title 50, United States Code, Sections 1701 et seq., confers upon the President authority to impose

economic sanctions in response to unusual and extraordinary threats to the national security and foreign policy of the United States when the President declares a national emergency with respect to any such threat. Section 1705 provides, in part, that "[i]t shall be unlawful for a person to violate, attempt to violate, conspire to violate, or cause a violation of any license, order, regulation, or prohibition issued under this chapter." 50 U.S.C. § 1705(a).

52. On June 26, 2008, pursuant to his authorities under IEEPA, the President issued Executive Order 13466, finding that the "existence and risk of the proliferation of weapons-usable fissile material on the Korean Peninsula constitute an unusual and extraordinary threat to the national security and foreign policy of the United States" and declaring a national emergency to deal with that threat. On March 15, 2016, in recognition of the "the Government of North Korea's continuing pursuit of its nuclear and missile programs" and to take additional steps with respect to the national emergency declared in Executive Order 13466, the President issued Executive Order 13722, blocking all property and interests in property that were then or thereafter came within the United States or the possession or control of any United States person, of the Democratic People's Republic of Korea ("DPRK" or "North Korea"), the Workers' Party of Korea ("WPK"), and any individual or entity determined by the Secretary of the Treasury, in consultation with the Secretary of State, to meet one or more enumerated criteria.

53. Executive Order 13722 prohibits, among other things, (i) the transfer, payment, exportation, withdrawal, or dealing in any property or interests in property in the United States or in the possession or control of any United States person of any person whose property and interests in property are blocked pursuant to the order; (ii) "the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any [such] person"; (iii) "the receipt of any contribution or provision of funds, goods, or services from any such person; (iv) "[a]ny transaction

that evades or avoids, has the purpose of evading or avoiding, causes a violation of, or attempts to violate any of the prohibitions set forth in this order"; and (v) "[a]ny conspiracy formed to violate any of the prohibitions set forth in this order."

54. To implement Executive Order 13772, OFAC amended the North Korea Sanctions Regulations, 31 C.F.R. Part 510, on March 5, 2018. These regulations incorporate by reference the prohibited transactions set forth in Executive Order 13722. *See* 31 C.F.R § 510.201. The regulations also provide that the names of persons designated pursuant to Executive Order 13722, whose property and interests are therefore blocked, are published in the Federal Register and incorporated into the Specially Designated Nationals and Blocked Persons ("SDN") List, which is published on OFAC's website. *Id.* Note 1.

55. On September 13, 2019, pursuant to Executive Order 13722, OFAC designated the hacking group commonly known within the global cyber security industry as the "Lazarus Group" as an SDN based on its relationship to North Korea's primary intelligence bureau. On April 14, 2022, OFAC identified as blocked property an ETH wallet address beginning with the characters 0x098B716 (the "0x098B716 Address") used by the Lazarus Group to launder stolen proceeds from the March 2022 Ronin Network hacking incident.

**The Ronin Network Hacking Incident**

56. On or about March 29, 2022, the Ronin Network, which administers a blockchain called the Ronin Blockchain, announced that there had been a security breach of a bridge it had developed to move cryptocurrency between the Ronin Blockchain and other cryptocurrency blockchains, including the Ethereum blockchain. The Ronin Blockchain is used for certain online video games, including Axie Infinity, an online non-fungible token-based video game. In its public announcement, the Ronin Network stated, in sum and substance, that hackers had obtained

unauthorized access to and control over five out of the nine validator nodes used to execute transactions on the Ronin Network bridge and had used this access and control to make unauthorized withdrawals of cryptocurrency from the bridge. As a result of this hack, the Ronin Network announced publicly that approximately $620 million worth of ETH and another cryptocurrency had been stolen.

57. The Tornado Cash founders were aware of the Ronin Network hack on the day that it was announced, and immediately recognized the likelihood that the hackers would use the Tornado Cash service to launder the proceeds. On or about March 29, 2022, ROMAN SEMENOV, the defendant, sent a message to ROMAN STORM, the defendant, and to CC-1 through the Encrypted App, saying "Have you seen a $600M hack today? Shit might seriously hit the fan now." SEMENOV then sent a link to a Tweet issued by the official Twitter account of the Ronin Network, describing the hack. Later that day, CC-1 sent a message to STORM and SEMENOV through the Encrypted App, saying "Heya, anyone around to chat about axie? Would like to ask a few general questions about how one goes about cashing out 600 mil."

58. Within days of the Ronin Network hacking incident and the above messages, the hackers began depositing the proceeds of the hack into the Tornado Cash service. In total, at least approximately $455 million worth of ETH traceable to the Ronin Network hack was laundered through the Tornado Cash service between at least approximately April 4, 2022 and at least approximately May 19, 2022.

59. ROMAN STORM, ROMAN SEMENOV, the defendants, and CC-1 were fully aware within days of the Ronin Network hack that the proceeds of the hack were in fact being deposited into the Tornado Cash service. For instance, on or about April 4, 2022, a reporter sent an email to an email address used by all three Tornado Cash founders asking for comment on the

Ronin Network hack, in which the reporter included a link to a blockchain analytics website and stated that "it appears that these hackers are trying to use Tornado.cash to launder stolen funds."

60. On or about April 14, 2022, the Federal Bureau of Investigation ("FBI") publicly attributed the Ronin Network hack to the Lazarus Group. On or about the same date, OFAC designated the 0x098B716 Address, which was then holding the majority of the proceeds of the Ronin Network hack, as blocked property of the Lazarus Group and updated the SDN List entry for the Lazarus Group.

61. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 were aware that OFAC had designated the 0x098B716 Address as blocked property of the Lazarus Group. On or about April 14, 2022, STORM sent SEMENOV and CC-1 a message through the Encrypted App with a link to a news article about the FBI's attribution of the Ronin Network hack to the Lazarus Group. In the message, STORM wrote: "guys we are fucked."

62. Following this message, ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 discussed a plan to change the Tornado Cash UI to block deposits directly from OFAC-designated addresses, so they could make a public announcement claiming that the Tornado Cash service was compliant with United States sanctions. However, as STORM, SEMENOV, and CC-1 well knew, this change to the UI was ineffective and could be easily evaded in the absence of any KYC procedures, transaction monitoring, or blockchain tracing. To evade the screen, a customer of the Tornado Cash service who was using an OFAC-designated address could simply transfer the funds to a new Ethereum address and then deposit the funds into the Tornado Cash service, using the UI. The purpose of the change was to mislead the public into believing that the Tornado Cash service complied with the law, while continuing to allow and profit from transactions in funds originating in the OFAC-designated 0x098B716 Address.

63. In proposing this plan, ROMAN STORM, the defendant, indicated to ROMAN SEMENOV, the defendant, and CC-1 that its purpose was to make a public announcement claiming that the Tornado Cash service was not violating the law. On or about April 14, 2022, STORM sent the following message to SEMENOV and CC-1: "the address has been added to the OFAC list – these hackers are using tornado, we need to tell everyone urgently that we do not let such individuals on the front." In a follow-up message, STORM wrote that "a guy got 5 years of incarceration for sanctions," in a likely reference to a former Ethereum developer who was sentenced on April 12, 2022, for conspiring to assist North Korea to evade sanctions.

64. On or about April 15, 2022, ROMAN STORM, ROMAN SEMENOV, the defendants, and CC-1 agreed to change the UI to block deposits directly from OFAC-designated addresses. On that date, the Tornado Cash founders issued a public Tweet announcing the change and stating that: "Maintaining financial privacy is essential to preserving our freedom, however, it should not come at the cost of non-compliance." However, in their private chats, the Tornado Cash founders indicated to each other that they understood that this screen would not be effective. On or about April 14, 2022, STORM sent a message to SEMENOV and CC-1 through the Encrypted App in which he stated that it would be "easy to evade" the new screen. The Tornado Cash founders also cautioned each other to avoid making further incriminating statements. On the following day, SEMENOV sent a message to STORM and CC-1 through the Encrypted App, saying that "regarding [Encrypted App] chats, we also have to bear in mind that law enforcement is reading them too and can use them against us later."

65. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 quickly learned that the screen they had implemented was in fact ineffective, as they had anticipated it would be. On or about April 16, 2022, the day after they had changed the Tornado Cash UI,

STORM sent SEMENOV and CC-1 a message through the Encrypted App with a link to a news article that described how the screen would not be effective in blocking continued money laundering through the Tornado Cash service by the Lazarus Group. The article described how the Lazarus Group was able to evade the screen on the Tornado Cash UI by transferring its ETH from the 0x098B716 Address for "a brief pit stop at a fresh, unsanctioned wallet, [and then] its crypto quickly flew through the popular coin mixer Tornado Cash, where the trail went cold."

66. Despite knowing that the screen they had implemented was ineffective in preventing the Lazarus Group's continued use of the Tornado Cash service to launder criminal proceeds, ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and CC-1 took no action to prevent the Tornado Cash service from facilitating this money laundering and sanctions evasion. In the absence of any such controls, the Lazarus Group continued to deposit tens of millions of additional dollars worth of proceeds of the Ronin Network hack from the 0x098B716 Address into the Tornado Cash service, by first moving the proceeds to one or more intermediate addresses.

67. ROMAN STORM and ROMAN SEMENOV, the defendants, and CC-1 well knew that the Tornado Cash service was continuing to launder proceeds of the Ronin Network hack held in the Lazarus Group's 0x098B716 Address. On or about April 30, 2022, SEMENOV sent a message to STORM and CC-1 through the Encrypted App with a link to a blockchain analysis showing that 15% of all of the deposits into the Tornado Cash service over the preceding three months had come from the Ronin Network hack. The analysis also showed that more than 90% of all the deposits into the Tornado Cash service for which a source could be identified during that same time period were attributable to criminal exploits.

68. These transactions continued for weeks, through at least on or about May 19, 2022.

Throughout this time period, the Tornado Cash founders continued to operate the Tornado Cash service and facilitate the Lazarus Group's money laundering and sanctions evasion, including by paying the U.S.-based web hosting service to continue to host the Tornado Cash website, continuing to maintain and keep the UI accessible to customers, and promoting the Tornado Cash service in public statements. Moreover, STORM, SEMENOV, and CC-1 maintained the relayer algorithm and the Relayer Registry, which allowed them to profit financially from the continued use of the Tornado Cash service by the Lazarus Group (and other hackers, money launderers, and sanctioned entities).

**The Defendants' Profits from the Operation of the Tornado Cash Service**

69. In or about December 2020, ROMAN STORM, ROMAN SEMENOV, the defendants, and CC-1 each received approximately 800,000 TORN tokens as part of the initial distribution of TORN tokens that the Tornado Cash founders designed. Their TORN tokens were initially "locked," meaning that they were nontransferable, for a period of one year. After one year, one-third of each of the Tornado Cash founders' tokens unlocked, making them freely transferable, and the remaining two-thirds were set to unlock at a linear rate over the next two years.

70. On or about December 1, 2021, shortly before one-third of the Tornado Cash founders' TORN tokens were set to unlock, ROMAN SEMENOV, the defendant, sent a text message to ROMAN STORM, the defendant, and CC-1 through the Encrypted App, saying, in part, that "it is important to pump Torn." In the same text message, SEMENOV discussed having an "auction" at which the Tornado Cash founders could "collect information … as to how much and at what price the folks are willing to pay."

71. According to transaction data and data taken from a public listing of cryptocurrency prices, TORN tokens traded at an average daily price of approximately $30 per TORN token in

January and February 2022. On March 2, 2022, Tornado Cash implemented the Relayer Registry, which, as described *supra*, paragraph 21, required Tornado Cash relayers to purchase TORN tokens in order to be chosen to process withdrawals through the UI. This led to a significant increase in the market price of TORN tokens. Between March 2, 2022 and April 30, 2022, TORN tokens traded at an average daily price of approximately $47 per TORN token.

72. Over the following months, ROMAN STORM, ROMAN SEMENOV, the defendants, and CC-1, continued to focus on increasing the profitability of the Tornado Cash service to increase the value of their holdings of TORN tokens and to appeal to potential investors in the Tornado Cash service. On or about June 16, 2022, STORM sent a message to SEMENOV and CC-1 through the Encrypted App in which he wrote "need help to push tornado to make some money / need to sell a sweet fantasy to investors."

73. At various times in 2022, ROMAN STORM, the defendant, sold TORN tokens that had been distributed to him and to ROMAN SEMENOV, the defendant, and CC-1. In an effort to conceal their sales of TORN tokens, STORM sold a portion of his, SEMENOV's, and CC-1's TORN tokens through an account held in the name of another person, a Russian national, at Binance, a cryptocurrency exchange (the "Binance account"). In fact, STORM personally executed transactions using the Binance account, and STORM, SEMENOV, and CC-1 had transferred TORN tokens to that account for the purpose of selling them without revealing those sales to the public, including to other holders of TORN tokens. On or about June 21, 2022, after the Ronin Network hacking incident described above, STORM sent a message to SEMENOV and CC-1 through the Encrypted App in which he stated that he had traded a quantity of TORN tokens for stablecoins pegged to the United States dollar. He further explained, in part, "I did everything from the Russian Binance … and even from a Russian IP (VPN)."

74. On or about August 8, 2022, OFAC announced the imposition of sanctions on the Tornado Cash service pursuant to Executive Order 13694. In its public announcement of sanctions, OFAC stated: "Tornado Cash has repeatedly failed to impose effective controls designed to stop it from laundering funds for malicious cyber actors on a regular basis and without basic measures to address its risks."

75. After the sanctions on the Tornado Cash service were announced, ROMAN STORM, the defendant, again accessed the Binance account, where he was holding at least approximately $8 million worth of cryptocurrency that represented the proceeds of sales of TORN tokens. On or about August 8 and 9, 2022, STORM transferred approximately $7.8 million worth of U.S.-dollar pegged stablecoins from the Binance account to three separate cryptocurrency wallet addresses in payments of approximately $2.6 million each. Each of these three wallets was owned by one of the Tornado Cash founders. On or about August 9, 2022, STORM sent messages through the Encrypted App to ROMAN SEMENOV, the defendant, and CC-1, saying "I offloaded 8,000,000 yesterday / I sent you guys 2.6 each." He then sent further messages advising SEMENOV and CC-1, in substance, to conduct further transactions to make it more difficult to trace these funds, saying "my personal advice: create new wallets, new seed phrases, transfer money to new addresses."

## STATUTORY ALLEGATIONS

### COUNT ONE
### (Conspiracy to Commit Money Laundering)

The Grand Jury charges:

76. The allegations contained in paragraphs 1 through 75 of this Indictment are repeated and realleged as if fully set forth herein.

77. From at least in or about September 2020 up to and including on or about August

8, 2022, in the Southern District of New York, and elsewhere, ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to violate Title 18, United States Code, Sections 1956(a)(1)(B)(i).

78. It was a part and an object of the conspiracy that ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and others known and unknown, knowing that the property involved in a financial transaction represented the proceeds of some form of unlawful activity, would and did conduct and attempt to conduct such a financial transaction, which transaction affected interstate and foreign commerce and involved the use of a financial institution which was engaged in, and the activities of which affected, interstate and foreign commerce, and which in fact involved the proceeds of specified unlawful activity, to wit, (i) computer fraud and abuse, in violation of Title 18, United States Code, Section 1030, and (ii) wire fraud, in violation of Title 18, United States Code, Section 1343, knowing that the transaction was designed in whole and in part to conceal and disguise the nature, the location, the source, the ownership, and the control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

(Title 18, United States Code, Section 1956(h).)

## COUNT TWO
**(Conspiracy to Operate an Unlicensed Money Transmitting Business)**

The Grand Jury further charges:

79. The allegations contained in paragraphs 1 through 75 of this Indictment are repeated and realleged as if fully set forth herein.

80. From at least in or about March 2022, up to and including on or about August 8, 2022, in the Southern District of New York and elsewhere, ROMAN STORM, the defendant,

ROMAN SEMENOV, the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, operation of an unlicensed money transmitting business, in violation of Title 18, United States Code, Sections 1960(b)(1)(B) and (b)(1)(C).

81. It was a part and an object of the conspiracy that ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and others known and unknown, would and did knowingly conduct, control, manage, supervise, direct, and own all and part of an unlicensed money transmitting business, which affected interstate and foreign commerce, and (i) failed to comply with the money transmitting business registration requirements under Section 5330 of Title 31, United States Code, and regulations prescribed under such section, and (ii) otherwise involved the transportation and transmission of funds that were known to the defendants to have been derived from a criminal offense and to be intended to be used to promote and support unlawful activity, to wit, STORM and SEMENOV conducted, controlled, managed, supervised, directed, and owned all or part of the Tornado Cash service, a business that transferred funds on behalf of the public, without meeting the Federal registration requirements set forth for money transmitting businesses, and knowing that the business involved the transportation and transmission of funds that were derived from a criminal offense and were intended to be used to promote and support unlawful activity.

Overt Act

82. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt act, among others, was committed in the Southern District of New York and elsewhere: On or about May 1, 2022, ROMAN STORM, the defendant, transferred funds from a

corporate bank account held in a bank located in the Southern District of New York to a web hosting service to pay for hosting the Tornado Cash website.

(Title 18, United States Code, Section 371.)

**COUNT THREE**
**(Conspiracy to Violate the International Emergency Economic Powers Act)**

The Grand Jury further charges:

83. The allegations contained in paragraphs 1 through 75 of this Indictment are repeated and realleged as if fully set forth herein.

84. From at least on or about April 14, 2022, up to and including on or about August 8, 2022, in the Southern District of New York, and elsewhere, ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and others known and unknown, knowingly and willfully did combine, conspire, confederate, and agree together and with each other to violate orders, regulations, and prohibitions in and issued under the International Emergency Economic Powers Act ("IEEPA"), codified at Title 50, United States Code, Sections 1701 et seq., Executive Order 13722, and 31 C.F.R. § 510.201.

85. It was a part and an object of the conspiracy that ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and others known and unknown, would and did knowingly and willfully receive, and cause others to receive, funds, goods, and services from the Lazarus Group, a sanctioned entity, to wit, transfers, payments, deposits, and fees from the 0x098B716 Address, which constituted blocked property and interests in property of the Lazarus Group, without first obtaining the required approval of OFAC, in violation of 50 U.S.C. § 1705(a), Executive Order 13722, and 31 C.F.R. §§ 510.201.

86. It was further a part and an object of the conspiracy that ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and others known and unknown, would and did

knowingly and willfully provide, and cause others to provide, funds, goods, and services to, by, and for the benefit of the Lazarus Group, a sanctioned entity, to wit, transfers, payments, money transmitting services, and money laundering of funds in the 0x098B716 Address, which constituted blocked property and interests in property of the Lazarus Group, without first obtaining the required approval of OFAC, in violation of 50 U.S.C. § 1705(a), Executive Order 13722, and 31 C.F.R. §§ 510.201.

87. It was further a part and an object of the conspiracy that ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and others known and unknown, would and did knowingly and willfully transfer, pay, withdraw, and deal in and cause others to transfer, pay, withdraw, and deal in blocked property and interests in property of the Lazarus Group, a sanctioned entity, to wit, the 0x098B716 Address, in violation of 50 U.S.C. § 1705(a), Executive Order 13722, and 31 C.F.R. §§ 510.201.

88. It was further a part and an object of the conspiracy that ROMAN STORM, the defendant, ROMAN SEMENOV, the defendant, and others known and unknown, would and did knowingly and willfully engage in transactions to evade and avoid, and attempt to evade and avoid, the requirements of U.S. law with respect to the transfer, payment, withdrawal, and dealing in the 0x098B716 Address, which constituted blocked property and interests in property of the Lazarus Group, and the provision of funds, goods, and services by, to, or for the benefit of, and the receipt of funds, goods, or services from, the Lazarus Group, a sanctioned entity, without first obtaining the required approval of OFAC, in violation of 50 U.S.C. § 1705(a), Executive Order 13722, and 31 C.F.R. §§ 510.201.

(Title 50, United States Code, Section 1705; Executive Order 13722; 31 C.F.R. § 510.201.)

## FORFEITURE ALLEGATIONS

89. As a result of committing the offenses alleged in Counts One and Two of this Indictment, ROMAN STORM, the defendant, and ROMAN SEMENOV, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(1), any and all property, real and personal, involved in said offenses, or any property traceable to such property, including but not limited to a sum of money in United States currency representing the amount of property involved in said offenses.

90. As a result of committing the offense alleged in Count Three of this Indictment, ROMAN STORM, the defendant, and ROMAN SEMENOV, the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, any and all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of said offense, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offense that the defendants personally obtained.

91. If any of the above-described forfeitable property, as a result of any act or omission of the defendants: (a) cannot be located upon the exercise of due diligence; (b) has been transferred or sold to, or deposited with, a third person; (c) has been placed beyond the jurisdiction of the Court; (d) has been substantially diminished in value; or (e) has been commingled with other property which cannot be subdivided without difficulty; it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p) and Title 28, United States Code, Section

2461(c), to seek forfeiture of any other property of the defendants up to the value of the above forfeitable property.

(Title 18, United States Code, Section 981;
Title 18, United States Code, Section 982;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)

[redacted]

DAMIAN WILLIAMS
United States Attorney