

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Alexandria Division

UNITED STATES OF AMERICA,

Plaintiff,

v.

APPROXIMATELY 23,067,340 USDT
SEIZED FROM THE TETHER OPERATING
WALLETS SET FORTH IN ATTACHMENT
A,

and

APPROXIMATELY 5,011.03 BNB SEIZED
FROM A BINANCE D/B/A NEST
SERVICES LTD. ACCOUNT WITH USER
ID XXXX5216,

Defendants *in Rem*.

Civil No. 1:26-cv-_____

VERIFIED COMPLAINT FOR FORFEITURE *IN REM*

COMES NOW the plaintiff, United States of America, by and through counsel, and brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

NATURE OF THE ACTION

1. The United States brings this action *in rem* seeking the forfeiture of all right, title, and interest in the defendants *in rem* identified in the case caption above (collectively, the “Defendant Property”).

2. The United States’ claim arises from a concealment money laundering conspiracy carried out by the operators of Garantex, a sanctioned Russian cryptocurrency exchange. At times, Garantex failed to obtain know-your-customer (“KYC”) information. At other times,

Garantex obtained KYC information, but its operators nonetheless continued to allow transactions involving known criminal proceeds. Garantex was a favored cryptocurrency exchange for cybercriminals and cybercrime organizations, including those involved in ransomware, hacking, and terrorism financing, among others. The Defendant Property was contained within Garantex operating wallets that facilitated Garantex's operations. And as described in more detail below, Garantex consistently pooled the criminal proceeds it held with non-criminal proceeds with the purpose of disguising the nature, location, source, ownership, and control of those criminal proceeds.

3. The Defendant Property constitutes property involved in violations of 18 U.S.C. § 1956(h) (conspiracy to commit concealment money laundering) and is therefore subject to forfeiture pursuant to 18 U.S.C. § 981(a)(1)(A).

4. In summary, this complaint seeks forfeiture of instrumentalities used by a sanctioned Russian cryptocurrency exchange to provide services, aid, and resources to other cybercriminals throughout the world.

THE DEFENDANTS IN REM

5. Defendant approximately 23,067,340 USDT (Tether) was seized from 91 operating wallets set forth in Attachment A to this complaint on or about May 2, 2025, and subsequently was transferred to a cryptocurrency wallet controlled by the United States Secret Service ("USSS") on or about August 12, 2025.

6. Defendant approximately 5,011.03 BNB (Binance Coin) was seized from a Binance d/b/a Nest Services Ltd. Account with user ID XXXX5216 on or about July 23, 2025, and subsequently was transferred to a USSS-controlled cryptocurrency wallet in two transactions on or about September 30, 2025, and on or about October 7, 2025.

7. The property described in paragraphs 5 and 6 above are collectively the Defendant Property. The Defendant Property is currently in the possession of the USSS in Washington, D.C.

JURISDICTION AND VENUE

8. This Court has subject matter jurisdiction over actions commenced by the United States under 28 U.S.C. § 1345, and over forfeiture actions under 28 U.S.C. § 1355(a) and (b).

9. This Court has *in rem* jurisdiction over the defendant property under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia. The Court also has *in rem* jurisdiction over the defendant property under 28 U.S.C. § 1355(b)(1)(B) and 18 U.S.C. § 981(h) because defendants are charged criminally in Eastern District of Virginia case no. 1:25-cr-39 with an offense that is also the basis of this civil forfeiture action.

10. Venue is proper within this judicial district under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia. Venue is also proper in this district under 28 U.S.C. § 1355(b)(1)(B) and 18 U.S.C. § 981(h) because defendants are charged criminally in Eastern District of Virginia case no. 1:25-cr-39 with an offense that is also the basis of this civil forfeiture action.

FACTUAL ALLEGATIONS

11. Garantex was a Russian-operated cryptocurrency exchange that is the subject of sanctions issued by Department of Treasury's Office of Foreign Asset Control ("OFAC"). Garantex was routinely used to both facilitate and launder the proceeds of criminal activity, including ransomware, computer hacking, narcotics transactions, and sanctions violations. The administrators of Garantex were aware that Garantex was used for these purposes, actively avoided

preventing such activity, and profited from such activity. For example, Garantex failed to conduct basic know-your-customer (“KYC”) / anti-money laundering (“AML”) checks on its customers and thereby continued to provide a means for criminal organizations to launder illicit funds. When Garantex did identify criminal activity on its platform, it failed to take prompt remedial measures and instead continued to allow its platform to be used for criminal ends. Additionally, Garantex deliberately restructured its business operations to evade, and cause violations of, U.S. sanctions and to render it more difficult for law enforcement—as well as financial institutions and other third parties obligated to comply with OFAC and Financial Crimes Enforcement Network (“FinCEN”) regulations—to detect and block transactions with Garantex.

12. Garantex administrators intentionally designed and operated their business to enable criminals to launder their criminal proceeds, including proceeds from sanctions violations, and thus operated a money laundering enterprise. On or about February 27, 2025, two Garantex executives were indicted for their roles operating Garantex. Specifically, both Aleksej Besciokov and Aleksandr Mira Serda were indicted in case no. 1:25-cr-39.¹ The indictment included a count charging conspiracy to commit money laundering, in violation of 18 U.S.C. § 1956(a)(1)(B)(i), based on Besciokov, Serda, and others using Garantex as a means of laundering the proceeds of various unlawful activities, including ransomware, computer hacking, narcotics distribution, and sanctions violations, in violation of 18 U.S.C. §§ 1030 and 1343, 21 U.S.C. § 846, and 50 U.S.C. § 1705. On or about March 6, 2025, the U.S. Secret Service seized Garantex’s domains and completed administrative forfeiture of those domains on or about June 12, 2025. As explained herein, the Defendant Property facilitated Garantex’s money laundering activity by concealing and disguising the proceeds of criminal offenses and is therefore subject to forfeiture as property

¹ The U.S. government has subsequently been informed that Besciokov has died.

involved in Garantex's money laundering.

I. General Overview

13. Garantex was founded in late 2019 and operated primarily from its website hosted at garantex.io, while also maintaining accounts on social media platforms, such as Telegram. On its website, Garantex advertised the ability to carry out transactions for conversions of cryptocurrency to cryptocurrency, cryptocurrency to fiat currency, and fiat currency to cryptocurrency. Funds could be exchanged in the fiat currencies of Russian Rubles, U.S. Dollars, and Ukrainian Hryvnia. Cryptocurrencies that could be exchanged included BTC (Bitcoin), USDT (Tether), ETH (Ether), and several others. Garantex claimed that customers could withdraw funds at offices in Moscow and St. Petersburg, Russia, as well as a network of partner offices across Russia, Ukraine, and around the world. Garantex claimed to take a fee of approximately 0.1% to 0.2% of each transaction, depending on the nature of the transaction. Following OFAC sanctions in or around April 2022, Garantex began operating primarily from websites hosted at garantex.org and garantex.academy. Domains ending in .org use infrastructure maintained by Public Interest Registry of Reston, VA, and .academy domains use infrastructure maintained by Identity Digital of Bellevue, WA.

14. Garantex has stated on its website that customers were not permitted to make or participate in transactions on the Garantex platform or use any of Garantex's services if the user was a resident or citizen of the United States or if the user was named on either the U.S. Department of the Treasury's Specially Designated Nationals and Blocked Persons List or the U.S. Department of Commerce's Entity List. The terms of service also stated that before allowing a user to make a deposit to a Garantex website and at any time, Garantex could collect certain personally identifiable information such as a photo of a user holding a government-issued photo identification

document or similar documents.

15. In or around February 2022, Garantex lost its Estonian license to provide digital currency services after supervision by Estonia's financial regulatory authority revealed critical anti-money laundering deficiencies and found connections between Garantex and digital currency wallets used for criminal activity. Nonetheless, Garantex continued to offer services without meaningfully improving its anti-money laundering practices.

16. On or about April 5, 2022, OFAC sanctioned Garantex.² The OFAC press release noted that the majority of Garantex's operations were carried out in Russia, including at Federation Tower in Moscow, where other sanctioned digital currency exchanges have also operated. The press release indicated that over \$100 million in Garantex transactions were associated with illicit actors and darknet markets, including nearly \$6 million from the Russian ransomware actors behind Conti ransomware, and approximately \$2.6 million from Hydra, a Russia-based darknet market.³ OFAC's press release further put Garantex on notice of the fact that its services had been used for assorted criminal activity and that it was subject to U.S. sanctions.

II. Overview of Garantex's Facilitation of Illicit Activity and Money Laundering

17. Garantex has been integral to facilitating and concealing a variety of criminal activity including ransomware, funds stolen by hacking, and terrorism financing. The following paragraphs provide an overview of how Garantex is used to commit, conceal, and promote the

² <https://home.treasury.gov/news/press-releases/jy0701> (last accessed August 6, 2026).

³ At the time sanctions were imposed on it, Garantex had facilitated an overall volume of at least \$2.4 billion in transactions of bitcoin alone since its launch in 2019.

aforementioned crimes.

A. Ransomware

18. Garantex has received significant volumes of funds originating from ransomware victims. For example, OFAC’s April 5, 2022, press release announcing sanctions on Garantex described how \$6 million of funds were funneled through Garantex from the Russian ransomware actors behind Conti ransomware.

19. For example, one non-U.S.-based victim of the Conti ransomware group was directed to make payment to a Bitcoin address in exchange for regaining access to their systems. On or about June 30, 2021, the victim received a decryptor⁴ from the attackers. The Bitcoin blockchain shows that on this same day, the aforementioned Bitcoin address received an approximate \$430,000 payment. Approximately \$170,000 thereof was subsequently transferred to Garantex.

20. Another U.S.-based victim attacked with Conti ransomware made a payment of approximately \$311,220 to another Bitcoin address on or about June 26, 2021. Approximately \$166,000 of that amount was subsequently transferred to Garantex. A February 2022 blog post by Chainalysis, a reliable cryptocurrency forensics company utilized by numerous law enforcement agencies, reported that Garantex had received at least \$10 million from ransomware strains Netwalker, Phoenix, CryptoLocker, and Conti from 2019 to 2021.⁵

21. Generally, ransomware actors transfer funds from their own wallets, through

⁴ In the context of ransomware, a “decryptor” is a piece of software provided by an attacker to a victim so that the victim can regain access to their encrypted systems. Ransomware attackers will typically only provide a decryptor to a victim after the victim makes a ransom payment.

⁵ <https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/> (last accessed July 22, 2026).

intermediate wallets, to professional money laundering services or exchanges that do not respond to law enforcement requests and do not follow anti-money laundering best practices in order to launder illicit proceeds, pay other actors involved in the ransomware attacks, and to conceal the control and ownership of the funds.

22. The imposition of the aforementioned sanctions on Garantex did not change these patterns or the use of Garantex by such actors. Since the imposition of sanctions, there have been numerous additional instances of ransomware funds being laundered through Garantex.

23. A report authored by representatives of Elliptic, a reliable cryptocurrency forensics company utilized by numerous law enforcement agencies, from in or around November 2023, noted that Garantex had received approximately \$10 million in payments from victims of the Black Basta ransomware group since early 2022.⁶

24. Furthermore, according to Chainalysis's Reactor tool, Garantex's overall incoming transaction volume had an "indirect exposure" to ransomware payments and ransomware groups amounting to approximately \$27.9 million (valued at the time of the transactions) between in or around February 2018 and in or around March 2025. Chainalysis's Reactor tool is software that facilitates blockchain investigation by providing attribution to cryptocurrency addresses, mapping complex transaction flows, and following cryptocurrency movements across different blockchains. The concept of "indirect exposure" refers to a measurement of deposits that ultimately originate from ransomware, but were not deposited directly from a ransomware address to a Garantex address and instead involved multiple intermediary addresses before the funds in question were

⁶ The original study can be found at <https://www.elliptic.co/blog/black-basta-ransomware-victims-have-paid-over-100-million> (last accessed August 6, 2026). Although the report focuses on a \$100 million overall figure allegedly generated by Black Basta, USSS held a separate conversation with Elliptic and determined the specific amount transferred to Garantex was approximately \$10 million.

deposited to Garantex. This type of calculation is typically more reliable in terms of quantifying overall ransomware deposits handled by Garantex than simply reviewing direct exposure, as ransomware organizations will not usually receive victim funds and then directly transfer those funds directly to an exchange like Garantex. Instead, ransomware payments will usually first flow through several intermediary addresses for various reasons, to include concealment techniques employed by the ransomware organization or simply due to the specific Bitcoin wallet software utilized by the organization, among other reasons.

25. With respect to indirect payments between ransomware organizations and Garantex, there have been multiple instances of Garantex handling ransomware deposits, including at least as recently as 2024 (prior to the website ceasing operations in March 2025). For example, on or about February 8, 2024, Garantex received an approximately \$226,000 deposit that originated from a wallet utilized by the Black Basta ransomware group to receive an approximately \$1 million ransom payment from a U.S. victim.

B. Network Intrusions

26. In or around June 2022, hackers stole \$105 million worth of digital currency from a U.S.-based blockchain network through a network intrusion. After the funds were stolen, the attackers used a sophisticated series of transfers to launder the funds and at least \$7.4 million were transferred to a digital currency exchange (“DCE 2”), which cooperates with law enforcement. The account receiving the \$7.4 million was registered to email address proforg@gmail.com and registered with the identifiers of Aleksej Besciokov, a known Garantex administrator, who was indicted in case 1:25-cr-39.

C. Illicit Activity

27. As noted in the previously referenced April 2022 OFAC press release, up until that

time, over \$100 million in transactions processed by Garantex were associated with illicit actors and darknet markets.

28. Both pre- and post-sanctions, Garantex processed large volumes of digital currency funds to and from multiple additional illicit sources, thus further indicating that Garantex failed to combat money laundering conducted on its platform. According to Chainalysis Reactor, a non-exhaustive list of examples of funds from darknet marketplaces or other criminal sources that Garantex processed includes the following:

- a. In or around March 2021 to in or around October 2023: approximately \$634,000 from and \$380,000 to Blacksprut, a Russian darknet market that specializes in drug sales.
- b. In or around March 2022: approximately \$380 from a known child sexual abuse material website.
- c. In or around December 2022 to in or around December 2023: \$24,000 from and \$155,000 to Kraken Market, a darknet market that specializes in drug sales.
- d. In or around September 2023: approximately \$280,000 from PM2BTC, a long-time professional Russian money laundering service advertised primarily on cybercrime forums and designated by FinCEN on or about September 26, 2024, as an entity of “primary money laundering concern” in connection with Russian illicit finance.

29. Indeed, compared to most exchanges with meaningful KYC/AML programs, Garantex allowed disproportionately higher volumes of illicit transactions on its platform, thus further indicating that Garantex knowingly facilitated funds transfers on behalf of multiple kinds of cybercrime organizations and services. For example, a 2023 annual report published by

Chainalysis⁷ noted that in one particular 60-day period prior to OFAC sanctioning Garantex on or about April 5, 2022, 6.1% of incoming funds deposited to Garantex originated from illicit sources, with an additional 16.1% of incoming deposits originating from sources categorized by Chainalysis as “risky.”⁸ According to Chainalysis, these percentages were significantly higher than legitimate, law-abiding centralized exchanges, with the latter as a whole receiving, on average, approximately 0.3% of incoming deposits originating from illicit activities during that same 60-day period—meaning Garantex had twenty times more incoming deposits from illicit sources as a percentage of its overall deposits than other exchanges. From 2019 to 2021, at least approximately 31% of all of deposits to Garantex were from illicit or risky sources.⁹

B. Garantex Administrators’ Awareness of Illegal Activity on its Platform

30. Garantex administrators knew that the platform was being used to launder a significant volume of funds from illicit and risky sources and provide services to criminal actors. Among other things, Garantex was sanctioned by the United States in or around April 2022 for facilitating illicit activity, putting it on notice that such activity was taking place on its platform. The other public reporting on Garantex discussed above also would have put it on notice about the criminal activity on its platform. Finally, at times, Garantex used monitoring software to track

⁷ Report available for download at <https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction/> (last accessed August 6, 2026).

⁸ According to the Chainalysis annual report, “[r]isky activity refers to transactions in which one or more counterparty addresses are associated with a risky entity, such as a high-risk exchange or gambling service. Legitimate activity refers to transactions in which one or more counterparty addresses are associated with entities that are not inherently criminal or risky, such as personal wallets or exchanges.”

⁹ <https://www.chainalysis.com/blog/2022-crypto-crime-report-preview-russia-ransomware-money-laundering/> (last accessed August 6, 2026).

high-risk transactions on its platform but nevertheless permitted twenty times more deposits from illicit sources as a percentage of overall deposits than legitimate exchanges.

31. Legitimate cryptocurrency exchanges attempt to implement robust AML and KYC programs on their platforms to combat illicit activities, such as money laundering or terrorism financing, and to ensure that they are complying with local laws and regulations in the jurisdictions in which they operate. As a result, legitimate exchanges have relatively low volumes and percentages of illicit activity occurring on their platforms, as noted above. The Garantex administrators, however, failed to implement such programs—despite having the tools to do so—and as a result, Garantex had both a high volume and percentage of illicit activity on the platform.

32. Garantex’s customer database, as well as accounts operated by the administrators of Garantex, confirm the intentionally deficient approach to KYC/AML by the platform’s administrators. The database and accounts show that Garantex’s administrators were actively aware that certain customers were engaged in criminal behavior, but nonetheless continued to provide services to those criminal customers. The following is a non-exhaustive list of examples:

- a. An account registered to username “Crypto_slava” actively engaged in transactions on Garantex from in or around February 2021, until in or around late 2023, despite the account having been flagged by Garantex administrators on or about August 4, 2022, as being involved in the laundering of cryptocurrency. Although Garantex implemented a temporary block on the account, that block was removed less than one month later, on or about September 9, 2022, and the user was able to continue trading through at least in or around 2023.
- b. Administrator notes from in or around 2023 for an account registered to “global.crypto44@proton.me” included numerous entries about possible dirty

funds and other problems, including a note reading, “blocked, Terrorism Financing 100%!!!” This note was apparently later reversed with a note reading “everything’s ok.” However, data from Software Company B, a blockchain software analytics company used by Garantex, for the account shows that it was engaged in high-risk activities, despite the administrator comments indicating otherwise.

- c. An account registered to `alice.spam@yandex.ru` was opened on or about October 6, 2023, and transacted only around that time. A Garantex administrator note about the account reads, “eth, btc from Terrorism Financing,” although there is a subsequent note that the funds are from a charitable organization. Another note indicates that the account was referred to compliance. The account was not verified, and at least one transaction occurred after that referral.

33. Garantex failed to flag terrorism-related transactions up until on or about April 1, 2022, as confirmed by copies of Garantex’s administrator databases obtained by USSS. Similarly, Garantex administrators did not start flagging for transactions related to child sexual abuse material or international sanctions, categorized in a tool offered by Software Company A, another blockchain software analytics company used by Garantex, as “child_exploitation” and “sanctions,” respectively, until on or about April 1, 2022. Garantex did not utilize any other provider to flag transactions.

34. Garantex had begun using Software Company A on or about March 19, 2019, and ceased using the company on or about April 6, 2022, and did not use any other transaction monitoring firm until on or about June 3, 2023, when it started using Software Company B. Starting on or about November 7, 2023, Garantex again switched providers and began to use a third software company to flag transactions by risk.

35. Even during the periods when Garantex did use tools to monitor and flag transactions, administrators did not block many transactions identified by Garantex's software as "high risk." While Garantex was using Software Company A's services, Garantex had access to a feature that provided Garantex with a risk scoring framework to automatically flag transactions as associated with illegal or risky activities. Software Company A's risk scoring feature could be self-customized to allow clients such as Garantex to tailor the tool according to the AML/KYC requirements for different regions or countries in which they operate. The risk score for any given transaction ranges from 0 to 1.000, with 1.000 being the highest. Between on or about May 16, 2019, and on or about April 6, 2022, approximately 15,000 incoming deposits to Garantex were flagged by Software Company A's tool as having a risk score of 1.000, the highest possible risk score. Of those transactions with the highest risk scores, only 247 (or 1.6%) were marked in Garantex transaction database logs as "rejected," 7 were notated as "suspected," 11 were marked as "fraudulent," and all remaining approximately 15,000 were marked as "accepted."

36. Likewise, from in or around June 2023 to in or around March 2024, while Garantex was using services from Software Company B and another blockchain analytics company, Software Company C, it received approximately 219 notifications that a deposit was flagged as having a risk score of 1.000. Of these flagged transactions, no transactions were marked as "rejected"—all 219 deposits had a status of "accepted."

37. Over a dozen of these 219 deposits went to Garantex Account No. XXX1134. Garantex administrators had made several notes about this account receiving funds from questionable sources, including accounts linked to money laundering, yet the account was still permitted to remain active.

C. Crypto Max Account

38. Aleksandr Mira Serda, a cofounder and one of the primary administrators of Garantex, operates another exchange known as “CryptoMax,” which relies on Garantex infrastructure to function. As previously noted, Mira Serda is presently under indictment in the Eastern District of Virginia in Case No. 1:25-cr-39 as part of his role in Garantex. On or about June 17, 2019, Mira Serda registered a Garantex account using email address max@cryptomax.ru—the domain of which corresponds to a website associated with CryptoMax—and assigned an account “nickname” of “All1177.” The CryptoMax account is notated in Garantex databases to be a “Trusted Exchanger,” a category utilized by Garantex administrators to notate when certain customer accounts belong to approved third-party exchangers that utilize Garantex’s platform for liquidity purposes, for example. Mira Serda’s CryptoMax account was one of the highest volume accounts on the Garantex platform, ranking fifth overall based on incoming bitcoin deposits, and receiving at least 19,000 deposits, totaling approximately \$71 million between on or about June 26, 2019, and on or about March 11, 2024. There were tens of thousands of wallet addresses associated with the account.

39. CryptoMax offered its services to the public from the website cryptomax.ru. This website offered interested parties the ability to undertake instant exchanges or conversions between different types of cryptocurrencies without the need to register an account. Although customers could have registered an account with the platform, they could also perform financial transfers without creating an account by merely providing an email address and a Telegram handle to finalize a transfer. In other words, transactions could be conducted anonymously, without the need for KYC/AML documentation or to provide information concerning the source, destination, or nature of the funds being transferred. As a result, CryptoMax served as an attractive option for criminals seeking to launder funds from illegal activities.

40. Of the first 200 of CryptoMax's deposit addresses at Garantex, which transacted between on or about June 26, 2019, and on or about February 13, 2021, there was direct exposure of 42.18 percent to darknet markets and 22.66 percent to "No KYC" exchanges, per Chainalysis Reactor. These numbers were much higher than would be expected from a legitimate exchange.

41. As described in further detail below, Garantex has been integral to facilitating and concealing a variety of criminal activity, including ransomware, funds stolen by hacking, and terrorism financing. The following paragraphs provide an overview of how Garantex was used to commit, conceal, and promote the aforementioned crimes, specifically sanctions violations.

III. Garantex's Efforts to Avoid Transaction Monitoring and Cause Sanctions Violations

42. Since being sanctioned by OFAC, Garantex has implemented an operating wallet infrastructure that is designed to avoid having its transactions and operations blocked by other digital currency exchanges and to cause sanctions violations.

A. USDT Is Essential to Garantex's Operations

43. It is common for digital currency exchanges such as Garantex to convert incoming customer funds and reserve assets, regardless of the digital currency type, to USDT in order to shelter the funds from price fluctuations given the fact that the value of most digital currency assets is highly volatile. This practice allows exchanges like Garantex to ensure that they have sufficient funds available to satisfy voluminous transactions on their platforms and to protect them from collapse following significant dips in prices.

44. USDT was thus vital to the continued business operations of Garantex and, by extension, its ability to facilitate illicit USDT transfers, to include causing entities such as DCE 5, a major FinCEN-registered digital currency exchange, to unwittingly violate OFAC sanctions, as discussed below. However, Garantex customers also used USDT specifically to launder proceeds

originating from crimes such as ransomware attacks, in which victim bitcoin payments would be converted to USDT, and sent to Garantex-controlled wallets on the Tron blockchain for further distribution. Accordingly, Garantex-controlled USDT wallets enabled the laundering and distribution of criminal proceeds.

45. Furthermore, USDT transfers accounted for the highest volume of transactions processed on Garantex's platform. Garantex, through an account that it operated on DCE 2, received USDT deposits totaling \$835 million between in or around August 2021 and in or around March 2022. Between in or around July 2019 and in or around June 2024, Garantex processed at least \$4 billion in USDT on the Ethereum blockchain, approximately \$1.7 billion of which occurred post-sanctions. Similarly, between in or around March 2021 and in or around June 2024, Garantex processed at least \$31 billion in USDT on the Tron blockchain, approximately \$27 billion of which occurred post-sanctions. In addition, the top 20 Garantex users of USDT on the Tron blockchain were responsible for engaging in transfers of at least \$14 billion since Garantex launched. In sum, USDT is a pivotal component of Garantex's business operations, allowing the exchange to move large amounts of value in furtherance of its money laundering enterprise.

B. Garantex Deliberately Changed the Operation of Wallet Infrastructure for USDT Assets

46. Garantex administrators know about OFAC's sanctions on the company. For example, in a communication on or about April 6, 2022—the day after OFAC sanctioned Garantex—a Garantex administrator requested servers from an international server provider explaining that Garantex had been added to the “OFAC SDN” list. Notably, on or about April 8, 2022, just days after the imposition of sanctions, Garantex administrators sent a mass email to Garantex customers specifically noting that OFAC had sanctioned Garantex but stating—in the subject line of the email—“Garantex is operating normally.” On or about April 14, 2022,

Garantex's Chief Marketing Officer participated in an interview posted to Garantex's YouTube channel discussing the imposition of sanctions.¹⁰

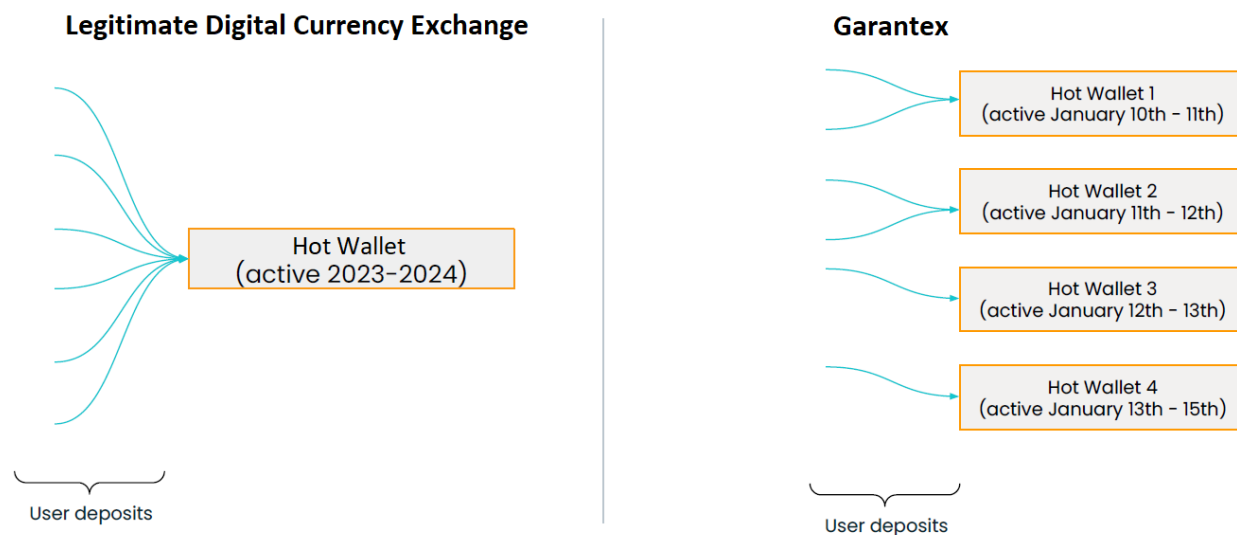
47. After U.S. sanctions were imposed on it, Garantex deliberately changed its business model and infrastructure practices to render it more difficult for financial institutions, such as other digital currency exchanges, to comply with U.S. sanctions by monitoring and blocking Garantex-performed transactions, as well as to render it more difficult for law enforcement to detect Garantex-performed transfers and seize Garantex-related funds. These changes ultimately have allowed Garantex to continue its participation in the financial and cryptocurrency ecosystems surreptitiously and without fear of reprisal, isolation, detection, or disruption. Garantex implemented these changes across multiple different blockchain networks used to support currencies offered on its platform, including USDT.

48. The primary step taken by Garantex to counter third party transaction monitoring and blocking efforts involved changes to the platform's use of operational wallets, also referred to as "hot wallets." In the context of digital currency exchanges, operational wallets are exchange-operated wallets connected to the Internet that facilitate the overall customer transactions performed on the exchange platforms at any given time. For example, operational wallets are used for processing customers' internal trades (*i.e.*, USDT in the operational wallet can be sent to a customer seeking to exchange BTC for USDT), consolidating incoming customer deposits, and providing a funding source for the processing of customer withdrawals outside of the exchange platforms. Operational wallets function similarly to master treasury accounts at traditional financial institutions. The identification of an exchange's operational infrastructure is one of the primary methods that blockchain analysis and AML compliance companies use to attribute

¹⁰ <https://www.youtube.com/watch?v=Y68iFDD0ADY>.

transactions, addresses, and wallets to specific known exchanges such as Garantex.

49. Beginning in or around early 2023, Garantex sought to evade this standard tracing and detection function by changing its operational wallets, on average, on a daily basis. In or around February 2025, Garantex began changing its operational wallets even more frequently, sometimes only using specific operational wallets for no more than 20 minutes. This practice is inconsistent with that of a legitimate digital currency exchange similar to Garantex's size and is a departure from Garantex's practices before sanctions were imposed on it. There is no legitimate business reason for Garantex to continually replace its USDT operational wallet infrastructure outside of an intent to render it more difficult for financial institutions, as well as law enforcement, to detect, monitor, block, or seize its transactions. The following is a visual depiction of operational wallet transactions at legitimate digital currency exchanges versus Garantex:



50. Garantex's operational wallets were most active on the Tron network, with USDT comprising the vast majority—up to 99.1 %—of assets processed by these Tron operational wallets every day.

51. Despite Garantex's attempts to conceal its activities, law enforcement was able to identify Garantex's operational wallets and seize the funds from these wallets, which are identified

in Attachment A. These wallets contain defendant 23,067,340 USDT.

C. Garantex Induces U.S. Parties to Violate Sanctions

52. U.S. persons and entities are required to comply with U.S. sanctions. According to a March 2024 notice,¹¹ “[n]on-U.S. persons [and entities] are also subject to certain OFAC prohibitions. For example, non-U.S. persons [and entities] are prohibited from causing or conspiring to cause U.S. persons [and entities] to wittingly or unwittingly violate U.S. sanctions, as well as engaging in conduct that evades U.S. sanctions.” But Garantex caused U.S. parties to violate sanctions in at least two ways. First, Garantex continued to process transactions involving U.S. persons through in or around 2025, thereby providing unlawful services to U.S. persons. Second, Garantex caused sanctions violations by deliberately changing its operational wallet infrastructure so that otherwise compliant U.S. entities or exchanges were prevented from detecting that they are entering into transactions with Garantex.

53. For example, a U.S.-based digital currency exchange (“DCE 1”) identified multiple transfers between U.S.-based customers of DCE 1, including customers located in the Eastern District of Virginia, and addresses associated with Garantex. At least 131 of these transactions with U.S.-based customers occurred from in or around April 2022, when Garantex was sanctioned, to in or around March 2024.

54. Another major FinCEN-registered digital currency exchange (“DCE 5”) has similarly transacted with Garantex since Garantex was sanctioned. DCE 5 has a relatively mature transaction compliance program. DCE 5 and Garantex engaged in over 5,800 transactions with one another involving USDT on the Tron network between when OFAC sanctioned Garantex in or around April 2022 until in or around March 2025. These 5,800 transactions amounted to

¹¹ <https://www.justice.gov/opa/media/1341411/dl?inline>

approximately \$50 million in USDT sent from DCE 5 to Garantex and approximately \$38 million in USDT sent from Garantex to DCE 5 since sanctions were imposed.

55. Similarly, DCE 5 and Garantex have engaged in over 540 transactions with one another involving USDT on the Ethereum network since OFAC sanctioned Garantex until in or around September 2024. These 540 transactions amounted to approximately \$3.9 million in USDT sent from DCE 5 to Garantex and approximately \$2.1 million in USDT sent from Garantex to DCE 5 since the imposition of sanctions.

56. Entities such as DCE 5 would typically have the ability to block a significant portion of transactions with a sanctioned entity and would comply with their legal obligation to do so. But DCE 5 permitted these transactions because it did not realize it was transacting with Garantex, at least in part because of Garantex's efforts to conceal its ownership of its operational wallets.

D. Garantex Statements Concerning USDT and Sanctions Circumvention

57. There was a Telegram channel registered to username @garantex_chs and administered by username @eugyyb. This account was operated by Garantex's Chief Marketing Officer. Another administrator in the @garantex_chs channel had username @Bonqai. @Bonqai was the Telegram handle associated with a designated Garantex administrator account. In other words, Telegram channel @garantex_chs and the account @Bonqai were operated by Garantex leadership. The contents and broadcasted messages of this channel revealed a public posting by @Bonqai dated on or about December 10, 2023, which noted, in Russian, the following:

"Tether only blocks wallets included in the OFAC list, currently there is only 1 wallet on this list, used by Garantex before April 2022 with a balance of 0, not a single Garantex wallet used after April 2022 is on the list [...] Adding wallets to this list is a slow bureaucratic process that lags significantly behind Garantex's current business processes [...] We closely monitor the global situation and constantly improve our work so that our clients can work peacefully [...] Blocking

wallets without significant legal grounds is a critical threat to Tether's reputation and business, so the list of blocked wallets will expand slowly and with a long delay."

The above posting indicates that the Garantex leadership actively monitored the actions of OFAC and other authorities to create an environment in which its Tether / USDT infrastructure remained undetected so that its customers could transact and trade on its platform without interference. The posting also indicated that the administrators of Garantex believed that if they do not use the same wallet addresses on a recurring basis, OFAC would be unable to sanction their addresses or block transactions. In other words, this posting helps confirm that Garantex's daily wallet changes were in fact designed to make it more difficult for other institutions and the U.S. government to detect and prevent its transactions.

E. Garantex's Reactions to Public Reporting Indicate that Garantex Leadership Is Aware of Its Role In Evading Sanctions and Laundering Money

58. In addition to causing sanctions violations by unknowing parties, public reporting has suggested that Garantex offered a means by which Russian businesses intentionally evade U.S. sanctions. For example, in a Wall Street Journal article dated on or about April 1, 2024, a Russian arms smuggler, Andrey Zverev, boasted about evading sanctions restricting arms sales, explained that he would do so by using Tether, and stated that his preferred trading platform for using Tether was Garantex. In a blog post, Zverev explained that "the evil regulators' in the U.S. and Europe wouldn't be able to shut Garantex down."

59. The Wall Street Journal article reported that a Garantex spokesperson denied that the exchange facilitates criminal activities but noted that Garantex "*appreciated Zverev 'giving a high appraisal of our services.'*" A corporate spokesperson for a legitimate business that is not interested in facilitating criminal activity would not welcome the endorsement of a known international arms dealer, but this statement is indicative of Garantex's intent to facilitate such

activity. Indeed, according to the article, Garantex's founder, Sergey Mendelev, had convened a meeting of key players in the cryptocurrency business in or around April 2023 to discuss solutions to the challenges faced by Russian military importers impacted by U.S. sanctions.

IV. Garantex's Use of 91 Tether Wallets Containing the Defendant 23,067,340 USDT to Facilitate Money Laundering and Sanctions Violations

60. In order for Garantex to provide exchange services, it requires an operating wallet infrastructure containing pools of different cryptocurrencies. The defendant 23,067,340 USDT consisted of the funds in some of Garantex's Tether operating wallets, which consisted of Tether stored on the Ethereum blockchain and Tether stored on the Tron blockchain, both of which are essential for the functioning of the exchange. During the period from on or about March 3 to on or about March 6, 2025, the cryptocurrency in the addresses identified in Attachment A were frozen so that funds could not be transferred out of these addresses. At the end of this process, approximately 91 Tether operating wallet addresses utilized by Garantex had been frozen. The group of frozen wallets included wallets operating for different durations spanning from just 20 minutes to multiple days.

61. Incoming customer deposits at Garantex—regardless of asset type—are immediately consolidated into operating wallets upon receipt, such as the wallets at issue here which contained the defendant 23,067,340 USDT. As a result, illicit transfers deposited into Garantex by customers are mixed in with the exchange's other funds. Illicit funds thus help provide liquidity for all transactions, and illicit transactions are facilitated—and hidden—by the entire pool of funds contained within Garantex's operating wallets. Accordingly, the funds in Garantex's operating wallets, such as the defendant 23,067,340 USDT, are likely a mix of funds derived from criminal activities, funds whose origins cannot be identified, and funds that may not be derived from criminal activities that are used to help conceal the nature and origin of the funds

derived from criminal activities. These funds were thus all involved in and facilitated Garantex's operations including its above-described money laundering activities, which included the laundering of proceeds of illegal activities relating to ransomware, computer hacking, narcotics distribution, child sexual abuse material, terrorism financing, and sanctions violations.

62. TRM Labs's blockchain analytics software, which law enforcement has found to be reliable, indicated that many of the 91 Tether operating wallets from which the defendant 23,067,340 USDT was seized had transactional connections to illicit services and activities. For example:

- a. Blockchain analysis on one particular frozen address, 0xCB5dE9175721050C5A5cFfB6851Af1b6Dd081Eaf, revealed that the address was active between on or about March 4, 2025, and on or about March 5, 2025, and engaged in approximately \$1.29 million in transactions, at least \$75,000 of which involved indirect exposure to addresses that had been flagged as associated with financial scams.
- b. Analysis of another frozen address, TJGBCviPKtaTdY1Nk7S7TGHVBNjRAAdFM8f, revealed that the address was active between on or about March 1, 2025, and on or about March 3, 2025, and engaged in approximately \$14.4 million in transactions, at least \$23,000 was noted to have an indirect exposure to addresses associated with banned or controlled substances and violent extremism.
- c. Another frozen address, 0x0C5bF6e284858d96d2fD6Fb0d1B40347bfbeAeA8, was active between on or about February 24, 2025, and on or about March 3, 2025, engaged in approximately \$1.51 million in transactions, and had a direct exposure

of approximately \$91,000 to “blocklisted” addresses, which are assets that had previously been neutralized by administrating parties (e.g. Tether Holdings’ ability to freeze Tether addresses) because of criminal associations and which are no longer accessible to threat actors.

d. Frozen address TL1EGyHiNSPAWktmgb8kNavSCfzQg8aSDP was active between on or about February 28, 2025, and on or about March 3, 2025, and engaged in approximately \$140,000 in transactions. The addresses with which it transacted had separately been flagged as associated with investment fraud, hacked or stolen funds, various types of consumer complaints, and banned or controlled substances, further confirming that Garantex was not performing adequate inquiries in the nature of transactional counterparties.

e. This similarly holds true for another frozen address, TFSs1G4sNF3Ak3FmP1uXi3ZVtgqWZLGQJq, which was active between on or about February 24, 2025, and on or about March 3, 2025, engaged in approximately \$1.4 million in transactions, and transacted with other addresses that had historically been flagged as directly tied to child exploitation and human trafficking.

63. Overall, the 91 frozen addresses from which the defendant 23,067,340 USDT was seized collectively engaged in approximately \$331 million worth of transactions between in or around January 2024 and up until the freezes in or around March 2025. At least \$5 million thereof had direct or indirect exposure to various types of illicit services. Another \$3.5 million was flagged by Chainalysis Reactor to have direct and indirect exposure to high-risk services (e.g., other exchanges that do not require AML / KYC checks in order to create accounts).

64. To summarize, Garantex relied heavily on Tether operating wallets to conduct its business, and Garantex's reliance on Tether enabled the exchange to facilitate money laundering and to violate U.S. sanctions. Further, as noted above, Garantex consistently pooled illicit and non-illicit funds in its operating wallets for the purpose of concealing and disguising the nature, location, source, ownership, and control of the illicit funds.

V. 5,011.03 BNB Seized from Garantex's Operating Account at Binance Associated with User ID XXXX5216

65. A Binance, D/B/A Nest Services Limited ("Binance") account associated with user ID XXXX5216 was registered to Stanislav Drugalev, a founder and former executive of Garantex who died in or around February 2021. This account was registered on or about January 14, 2018, to the same email address used by Drugalev as part of his registration in Garantex databases, and included a copy of Drugalev's Russian passport and a photograph of Drugalev. The account was last accessed on or about January 28, 2025, suggesting that others had access to the account following Drugalev's death. However, the Binance account associated with user ID XXXX5216 ("Binance XXXX5216") has had no transactions since in or around February 2021. The contents of Binance XXXX5216 were seized by law enforcement on or about July 23, 2025, consisting of the defendant 5,011.03 BNB. Law enforcement seized the account's contents pursuant to a seizure warrant issued by a United States Magistrate Judge.

66. Binance XXXX5216 was an operational account used by Garantex for liquidity purposes. Specifically, in order for Garantex to provide exchange services, it sometimes relied on liquidity from other exchanges. For example, between in or around July 2019 and in or around June 2020, the CryptoMax account, which was operated by Garantex administrator Mira Serda, utilized an Application Programming Interface ("API") offered by Binance to use Binance

XXXX5216 to access Binance's platform and immediately transfer to the CryptoMax account on Garantex any incoming bitcoin payments received by Binance XXXX5216. This model, whereby one exchange, like CryptoMax/Garantex, operates off the infrastructure of another larger exchange, like Binance, is referred to as a "nested" relationship, in which CryptoMax/Garantex is referred to as a "nested exchange" that maintains a "nested account" at Binance. Indeed, Mira Serda's CryptoMax account was one of the primary Garantex users that benefited from the liquidity and other features offered by Binance XXXX5216 through Binance. For example, of the 9,158 unique bitcoin deposits (totaling 3,012 BTC) to Binance XXXX5216 from in or around May 2019 to in or around July 2020, around 1,609 (totaling 645 BTC) were credited to CryptoMax on Garantex via API. This means that around 21% of the aforementioned 3,012 BTC in deposits were credited to CryptoMax.

67. CryptoMax used the Garantex platform to be able to utilize Binance XXXX5216. CryptoMax's use of Binance XXXX5216 demonstrated how Garantex integrated Binance XXXX5216 into its infrastructure. For example, the API output for a transaction occurring on or about February 13, 2020, involving a deposit to Binance address 1KWJGmHxZRP8i7Z9Ac3HZbFr11JiXycibf, assigned to Binance XXXX5216 was immediately transferred to Garantex address 34rUFahPUSubX2ibZ4YYC2imY7yduDhvDB, assigned to CryptoMax. In this particular example, the deposit was also flagged in Garantex systems as associated with a darknet market, yet the transaction was still permitted to be completed.

68. Furthermore, Binance XXXX5216 had over 11,000 instances between in or around December 2019 and in or around June 2020 of Dutch IP address 178.128.140.232 performing such actions as accessing Binance XXXX5216 and performing withdrawals from the account via Binance's API. This Dutch IP address is also tied to Garantex infrastructure. For example,

Garantex-controlled accounts at a U.S.-based Internet service provider, such as one registered to admin@garantex.io and operated by indicted criminal defendant Aleksej Besciokov, reflected IP activity from this same Dutch IP address during the same time period as Binance XXXX5216. Similarly, servers at the aforementioned Internet service provider that hosted Garantex's main operating wallets had multiple logins from the same Dutch IP address.

69. Garantex was using Binance's infrastructure via Binance XXXX5216 for a period from at least in or around June 2019 to in or around February 2021 in order to operate and effect transfers on behalf of the Garantex exchange.

70. Garantex also used other exchanges for this purpose. For example, Garantex also used an account in the name of Aleksej Besciokov at DCE 2 to operate a "nested exchange." Much like how that account was registered to Besciokov, Binance XXXX5216 was registered to Drugalev, a founder of Garantex, but operated for the benefit of Garantex more broadly.

71. The 5,011.03 BNB seized from Binance XXXX5216 was comprised of incoming deposits directly from Garantex's primary bitcoin wallets, which were associated with the cluster that corresponds to the root address sanctioned by OFAC in or around April 2022. Wallets that hold multiple addresses are commonly referred to by a "root address." A root address is one address within the wallet or cluster, often either the first address that is identified as belonging to the cluster or the first used (i.e., oldest) address in the cluster.

72. To summarize, Garantex relied heavily on Binance XXXX5216 to conduct its business between at least in or around June 2019 and in or around February 2021, and Garantex's reliance on Binance enabled Garantex to facilitate concealment money laundering of various unlawful activities including ransomware, computer hacking, and narcotics distribution. Further, as noted above, Garantex consistently pooled illicit and non-illicit funds in its wallets for the

purpose of concealing and disguising the nature, location, source, ownership, and control of the illicit funds.

COUNT 1
(Forfeiture Under 18 U.S.C. § 981(a)(1)(A)
as Property Involved in Transactions in Violation of 18 U.S.C. § 1956(h))

73. The United States incorporates by reference Paragraphs 1 through 72 of this complaint as if fully set forth herein.

74. Title 18, United States Code, Section 981(a)(1)(A) subjects to forfeiture “[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 . . . of this title, or any property traceable to such property.”

75. Title 18, United States Code, Section 1956(a)(1)(B)(i) imposes criminal liability on “[w]hoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity . . . knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.”

76. As set forth above, the Defendant Property contains proceeds of violations of specified unlawful activity, including proceeds of 18 U.S.C. §§ 1030 (fraud and related activity in connection with computers), 1343 (wire fraud), 2252 (certain activities relating to material involving the sexual exploitation of minors), and 2339C (prohibitions against the financing of terrorism); 21 U.S.C. § 846 (conspiracy to commit controlled substances offenses); and 50 U.S.C. § 1705 (sanctions evasion).

77. Title 18, United States Code, Section 1956(h) provides that, “[a]ny person who conspires to commit any offense defined in this section...shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.”

78. As set forth above, the Defendant Property constitutes property involved in violations of section 1956(h).

79. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

PRAYER FOR RELIEF

WHEREFORE, the United States requests that judgment be entered in its favor against the Defendant Property; that pursuant to law, notice be provided to all interested parties to appear and show cause why the forfeiture should not be decreed; that the Defendant Property be forfeited to the United States and delivered into its custody for disposition according to law; that the United States be awarded its costs and disbursements in this action; and for such and further relief as this Court may deem just and proper.

Dated: September 17, 2026

Respectfully submitted,

Todd W. Blanche
Attorney General

Theophani K. Stamos
First Assistant United States Attorney

By: /s/ Kevin Hudson
Kevin Hudson
Assistant United States Attorney
Virginia State Bar No. 81420
Attorney for the United States
11815 Fountain Way, Suite 200
Newport News, VA 23606
Office Number: (757) 591-4000
Facsimile Number: (757) 591-0866
Email Address: kevin.hudson@usdoj.gov

/s/
Stefanie Schwartz
Assistant United States Attorney
2100 Jamieson Avenue
Alexandria, Virginia 22314
Office Number: (703) 299-3734
Facsimile Number: (703) 299-3982
Email Address: Stefanie.Schwartz@usdoj.gov

/s/ Annie Zanobini
Annie Zanobini
Assistant United States Attorney
California Bar No. 321324
2100 Jamieson Avenue
Alexandria, Virginia 22314
Office Number: (703) 299-3903
Facsimile Number: (703) 229-3982
Email Address: annie.zanobini2@usdoj.gov

James Silver
Chief, Computer Crime and Intellectual Property
Section,
Criminal Division

By: /s/ Brian Mund
Brian Mund, Trial Attorney
Criminal Division, Department of Justice
1301 New York Avenue NW
Washington, DC 20005
Office Number: (202) 598-6205
Email Address: Brian.Mund@usdoj.gov

/s/ Tamara Livshiz
Tamara Livshiz, Trial Attorney
Criminal Division, Department of Justice
1301 New York Avenue NW
Washington, DC 20005
Office Number: (202) 674-5670
Email Address: Tamara.Livshiz@usdoj.gov

VERIFICATION

I, Willis Cheng, Special Agent, United States Secret Service, declare under penalty of perjury as provided by 28 U.S.C. § 1746, that the foregoing Complaint for Forfeiture *in Rem* is based on information known by me personally and/or furnished to me by various federal, state, and local law enforcement agencies, and that everything contained herein is true and correct to the best of my knowledge.

Executed at Washington, District of Columbia, this 16th day of September, 2026.

WCHENG Digitally signed by WCHENG
Date: 2026.09.16 15:37:49
-04'00'

Willis Cheng
Special Agent
United States Secret Service

ATTACHMENT A: OPERATING WALLETS

Tether Operating Wallet	Blockchain Network
TJGBCviPKtaTdY1Nk7S7TGHVBNjRAdFM8f	Tron
TEe7mhDCAduzWUXsxscyQqUV7AQooSTckL	Tron
TAabrsoK8Y2ANB8SJSEdbCus6Ha59fxGhc	Tron
TGGgCca1NoCbSXt1dNtKjXmVqqXnwrYkaK	Tron
TY8nvVKhn2ExTbphJ49RW17ULMKu9hm17n	Tron
TS6HNGuhFSrUZ4WGyrCtMfwgJe62BXvSEG	Tron
TLeLLfqe8dz2oQYgKXsiEFJAU3Xf4egoKN	Tron
TRov5UwFfJ7XNYyBypkHLvFS2xoPxGa18K	Tron
TMMXbo8F5EaPtVYe8EubE5wCqzWroxtVsY	Tron
TL1EGyHiNSPAWktmgb8kNavSCfzQg8aSDP	Tron
THajyUuFx9DY2ruQTgsdLkm3S8x5meiEzL	Tron
TQm4TzqWy2tbYX5wZ8i4AcPydCn5XHwPS5	Tron
TTfMJsMGJRvkx4BfpyfRzosGW73W5dNN6w	Tron
TRM6bdcy61hVwZKZWqHnSR1qhTCnPN1b65	Tron
TTiWBGQ5Y1M789aiskFhreTTQ3zfZrnQrT	Tron
TFSS1G4sNF3Ak3FmPluXi3ZVtgqWZLGQJq	Tron
TJoVnZtL8wJkiFYM8wNuv97rGzPWfHyomj	Tron
TDEsXLMmxSvX1js3xYCzLA6giDS78BN3Gb	Tron
TXwdGQKW3Xsf3y9eMsNySFViJKy1rTBsjG	Tron
TB5tyKz6Cpq6nCjDRPtzXTTGK3Pa7BYqCb	Tron
TH6o96B1WAokEtMyEMzBYwtYsiEEtwyxQc	Tron
TMSwSMnXXjHPoRM2Q2aJCowZYT6pSseSJ	Tron
TSxFYzM1S4YDoYFaGXEfyBSW7XSc7bXNN2	Tron
TDYEA5iFMgfAewqM6NhXkY3AhE5odUchV	Tron
TXFUjRdBj5A5MPSCteo7uzJPwHM6FbVdH	Tron
TC4jieJwuzbKeKVA4GBtd3ucz6LdGvWTSO	Tron
TJ3QjW1rSQRf3ktfDE7DpsfAS67T24GLjU	Tron
0xb271036d95b205A26bAe5cb2d4Eb922C000903A2	Ethereum
0x6614503a5a050c7d324731F57A35993e14c19E37	Ethereum
0xf6a25FCCF12320873555104465862f0d6E7d57d1	Ethereum
0xB09323411bbc6A2e3b03C2f4017Ec196748DD59c	Ethereum
0xc33a016022dC4d025306927024C52598aa0A384	Ethereum
0x997300928A3592736ab87A31bc2c473C79bF46d0	Ethereum
0xf12757E7F375347a2DD27a25C772b97DF64d8a17	Ethereum
0x0C5bF6e284858d96d2fD6Fb0d1B40347bfbeAeA8	Ethereum
0xD9d8B1d2337D6a63208e23019Aa02Cad369E1Ff1	Ethereum
0xc0488fb68d9094e37e6498e44069b3490a14d43f	Ethereum
0xEb28Ae1Bc8B9eF953355F288c8a31d6D9f6d9B4f	Ethereum
0x40d66b4328c835d0e5ad4751469f15d9085f0d24	Ethereum
0xe94f8337d6f739caa173bcb7fad2c11f89f5951b	Ethereum
0xf34ef00a2183cd762542f2885c123129f7a561ba	Ethereum

TUCUYfWvGDxxNPv2YFpLzDAKEGfiURU1h9	Tron
TVCVNxFchrEUPm5dPFt6ApRCHTMJBPWZpc	Tron
TB525xGAW9BUfyLA87mDD1AbD1MPwypeHx	Tron
TREG13XC5PC6tYtng hvuuiyDqDqvsWydAL	Tron
TVKc9JKuX64qB3JYBeNJZ9tgPVkdchcctW	Tron
TYTjg6VdmnbQbZfaX2pb3qaXW1mUYc7J6L	Tron
TQ5X3YsTi1NzSD23qUj5mcUcJPbfYteGGD	Tron
TWjqW79SiDFtZDYHwLarubL96EvV8HGwHz	Tron
TU7NLrBfY9T8RW37ncoo1UTjoK56ZJmzke	Tron
TES4TCD5FMCgoajcURmiW1RVB9a1xwSPj2	Tron
TAcR7zTMEFuEqd3PQGqe2RrnhsaPsyXi3w	Tron
TFpWAB7UceaW33RjZLxV2YgKC3nmNs2LAn	Tron
TWtx6nbGxb8MofjbADXX4i5heaH5eHAUJM	Tron
TCgduHb2WN23TDdhu5GSuEEhbjHJqu394o	Tron
TWWn7Vy5ZYEyco676grir3h61qLsW9H6Xx	Tron
TUnKy5TDpVAoozSXQdPyVT4sWbXDM1o4DN	Tron
TUJVwbw5Z7btGu7wsJWHaKJzJfn5wRahpR	Tron
TP4aXfmDkdFp81gK97TXaErCwJsZi8ks3q	Tron
TEBetd7ppKYESDWfiPbdJxC59MMibh8LJr	Tron
0xA9C71d9074B5a8c915CBc9078bEfDf0cb8E4480	Ethereum
TAueuMLKN2qfvFzMZ8ukziH7vkmoKgpSNB	Tron
TMkHn2fVE9nFUSSbyi7Mbdz54SAJZjwSYD	Tron
TKoiYr3xYWD3L9DqNfmnc6WNjRp9uE8XP2	Tron
0xe3a03672443cc48e9c5c0f667357734d4902551e	Ethereum
0x3ee372edf20782b16f8af94ec08e8d78ac00eb5c	Ethereum
0xBaA9c186a898C70fA70786aaF02f669f17Ed327b	Ethereum
TMSVCJYBCB5GUKP4TR8ja1MkGwAYRuDxuM	Tron
TV5wHPiGZyAkfwMzLvPoJgMpf9crxvCoLP	Tron
TVu25wmbrFaWpfYmsqxx5gpzQLFgequoaq	Tron
TEeQpqRKY4BguEL6x6pcfGrdQuhJe8mAvK	Tron
TDtNVrHfDAcRPxcRcWC7vi4TcfAFfTjjHi	Tron
TCjVabHyMwx52FvCa748DRomZovEBMqBPd	Tron
TH1vegjjZhHtr7R9qBJ6HmrSzUnUj51rTM	Tron
TGTmZQMVeBnmDJYdS6yQmGnT3VsDi589Ux	Tron
TF2nnB49qGHX1pDecgwhBttYga4UFzvUEb	Tron
TBkuXtEFTxwQmowPzbY29XDAh7JBDyPWHy	Tron
TAhZqWiwnHfsQ4aaHMNC4rNEYXgauCE75z	Tron
TDubMv5NMkVTPTLwF81KXPtaXv2ehM9rsh	Tron
TW7qWg7ENk9oRTw8fXCZpbkAeilw7FSaLb	Tron
TL2Ts8CiBNNzcqkqQfYZAnj8ADLGtxF13J	Tron
TMZrs19p2kAAv85VvnM4JvP2Wh1cAAJdzA	Tron
0xa93d78cAcca9B56E48BC20524a117c7519d713b7	Ethereum
0xa1aa49A68BC57EcF1f455eaDe17395933Ab0F9cd	Ethereum
0xCB5dE9175721050C5A5cFfB6851Af1b6Dd081Eaf	Ethereum
0xA3e73034a583dff0a17D4b01Ada679d6de6BB39	Ethereum

0x94087A5D6156F3EC9F00900E34378543713015a7	Ethereum
0xd0c66Ad3E0277A182833eCc051e4cc4Aa723bd8E	Ethereum
0x480c437379e34dBa27Db7fBec6eE971990E1f3Ae	Ethereum
0x126104F444aC5daEf35439796049a0Cbe9b1973d	Ethereum
TDcDKetTpuJbeX7vqmvidKG8Nma5vQrpFR	Tron