

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

UNITED STATES OF AMERICA

v.

ALEKSEJ BESCIOKOV,
a/k/a Aleksej Bešciokov,
a/k/a proforg,
a/k/a iram,

and

ALEKSANDR MIRA SERDA,
a/k/a Aleksandr Ntifo-Siaw,
a/k/a Aleksandr Ntifo Siao

Defendants.

Criminal No. 1:25-CR-39

Count 1: 18 U.S.C. § 1956(h)
Conspiracy to Commit Money Laundering

Count 2: 50 U.S.C. § 1705(a)
Conspiracy to Violate the International
Emergency Economic Powers Act

Count 3: 18 U.S.C. § 371
Conspiracy to Operate an Unlicensed Money
Services Business

Forfeiture Notice

Under Seal

INDICTMENT

February 2025 Term – at Alexandria, Virginia

1. Garantex is a cryptocurrency exchange whose operations are based in Moscow, Russian Federation. Beginning in and around at least June 2019, and continuing to the present, ALEKSEJ BESCIOKOV, a/k/a Aleksej Bešciokov, a/k/a proforg, a/k/a iram; ALEKSANDR MIRA SERDA, a/k/a Aleksandr Ntifo-Siaw, a/k/a Aleksandr Ntifo Siao; and others known and unknown to the grand jury operated Garantex to launder the proceeds of criminal activity, including ransomware, computer hacking, narcotics transactions, and sanctions violations, and profited from the laundering. Garantex offered its services to the public first through the website Garantex.io and then through Garantex.org. Garantex also misled law enforcement, including the Russian police, about the identities of its customers. Since April 2019, Garantex has processed at

least \$96 billion in cryptocurrency transactions.

2. Garantex was sanctioned by the United States Department of the Treasury's Office of Foreign Assets Control ("OFAC") on April 5, 2022, for its role in facilitating money laundering of funds from ransomware actors and darknet markets. Notwithstanding wide-spread publicity surrounding the sanctioning of Garantex and Garantex administrators' personal knowledge of the sanctions imposed on Garantex, BESCIOKOV and his co-conspirators violated those sanctions almost immediately by continuing to transact with U.S.-based entities for services and infrastructure supporting Garantex. By in and around early 2023, BESCIOKOV and his co-conspirators had also redesigned Garantex's operations to evade and violate U.S. sanctions and induce U.S. businesses to unwittingly transact with Garantex in violation of the sanctions. For example, Garantex moved its operational cryptocurrency wallets to different virtual currency addresses on a daily basis in order to make it difficult for U.S.-based cryptocurrency exchanges to identify and block transactions with Garantex accounts.

3. At times relevant to this Indictment, Garantex operated as a money transmitting business within the United States without registering with the Financial Crimes Enforcement Network ("FinCEN") as it was required to do.

General Allegations

At times relevant to this Indictment:

4. From in and around March 2019 to in and around late 2023, Garantex offered its services to the public through the website Garantex.io. From in and around late 2023 through the present, Garantex offered its services to the public through the website Garantex.org. Garantex also operated Garantex.Academy, an online cryptocurrency educational resource that provided interested parties with instructions on how to trade on the Garantex website.

5. BESCIOKOV was a citizen of Lithuania and resided in the Russian Federation. From in and around January 2019 to the present, BESCIOKOV was an administrator of Garantex. His responsibilities included obtaining and maintaining critical Garantex infrastructure, as well as reviewing and approving transactions.

6. MIRA SERDA was a citizen of the Russian Federation and resided in the Russian Federation and elsewhere outside the United States. MIRA SERDA was a co-owner of both Garantex and Fintech Corporation LLC, the entity operating Garantex.Academy. From in and around 2019 to at least in and around January 2022, MIRA SERDA was the Chief Commercial Officer of Garantex. MIRA SERDA has maintained administrator accounts on Garantex's platform that he used to create new accounts and assign customers to various categories. From in and around June 2019 to the present, MIRA SERDA operated an exchange called CryptoMax using Garantex's infrastructure that was one of the highest volume accounts on the Garantex platform.

7. The following definitions applied:

- a. "Virtual currencies" were digital representations of value that, like traditional coin and paper currency, functioned as a medium of exchange (i.e., they could be digitally traded or transferred and could be used for payment or investment purposes). Cryptocurrencies, like Bitcoin and Ether, were types of virtual currencies that relied on cryptography for security. Cryptocurrencies used algorithms, a distributed ledger known as a blockchain, and a network of peer-to-peer users to maintain an accurate system of payments and receipts.
- b. A "blockchain" was a digital ledger run by a decentralized network of computers referred to as "nodes." Each node ran software that maintained an

immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly recorded all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. There were many different blockchains used by many different virtual currencies. For example, bitcoin in its native state existed on the Bitcoin blockchain, while Ether existed in its native state on the Ethereum network.

- c. A "virtual currency address" was an alphanumeric string that designated the virtual location on a blockchain where virtual currency could be sent and received. A virtual currency address was associated with a virtual currency wallet.
- d. A "virtual currency wallet" (e.g., a hardware wallet, software wallet, or paper wallet) stored a user's public and private keys, allowing a user to send and receive virtual currency stored on the blockchain. Multiple virtual currency addresses could be controlled by one wallet.
- e. "Stablecoins" were a type of virtual currency whose value was pegged to a commodity's price, such as gold; to a fiat currency, such as the U.S. dollar; or to a different virtual currency. For example, USDT, also known as Tether, was a stablecoin pegged to the U.S. dollar that could be traded on the Ethereum and Tron blockchains, among others. Stablecoins achieved their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

- f. “Ransomware” was a type of malicious software program that encrypted contents of a victim computer or computer network and removed the ability for a victim to access the computer or computer network. In order for the victim to regain access to the computer or computer network, the victim had to pay a ransom, typically in bitcoin, to the attackers in exchange for receiving the required decryption keys.
 - g. “Darknet markets” were platforms used by criminals to buy and sell illicit goods, such as drugs. They sometimes also provided additional services to facilitate criminal activity, including serving as a payment intermediary or escrow agent for a criminal transaction. For example, if someone were to buy drugs using a darknet market, they could either transact directly with the drug dealer, or they could send the money to the forum administrator, who would ensure that the purchaser received the drugs before the dealer was paid.
- 8. All amounts of currency, dates, and times are approximate.
 - 9. BESCIOKOV and MIRA SERDA are expected to be first brought to and arrested in the Eastern District of Virginia.

COUNT ONE
(Conspiracy to Commit Money Laundering)

THE GRAND JURY CHARGES THAT:

- 10. Paragraphs 1 through 9 are hereby incorporated by reference.
- 11. From in and around June 2019 and continuing through the present, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendants, ALEKSEJ BESCIOKOV and ALEKSANDR MIRA SERDA, did knowingly and intentionally combine, conspire, confederate,

and agree with each other and others known and unknown to the Grand Jury to conduct and attempt to conduct a financial transaction, knowing that the property involved in the transaction represented the proceeds of some form of specified unlawful activity, and did in fact involve the proceeds of specified unlawful activity, to wit, violations of Title 18, United States Code, Sections 1343 and 1030; Title 21, United States Code, Section 846; and Title 50, United States Code, Section 1705, and knowing that the transaction was designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

Manner and Means of the Conspiracy

It was part of the conspiracy that:

12. Between in and around June 2019 through the present, BESCIOKOV, MIRA SERDA, and others operated Garantex as a means of laundering the proceeds of various unlawful activities, including, but not limited to, ransomware, computer hacking, narcotics distribution, and sanctions violations. For example:

- a. Between in and around 2021 and in and around 2024, Garantex laundered millions of dollars in ransomware proceeds, including proceeds from the Black Basta, Play, and Conti ransomware groups.
- b. In and around June 2022, Garantex laundered \$22 million in proceeds from the hack of a U.S.-based blockchain network, including through an account at a third-party exchange that was registered to BESCIOKOV and used to support Garantex's operations.
- c. Between in and around July 2022 and in and around April 2023, Garantex processed at least approximately \$2,570,000 from a Russian-speaking online criminal forum utilized by a variety of elite cybercriminals. Goods and services

offered for sale on this forum include malware such as ransomware and credentials that can be used to gain unauthorized access to networks and accounts.

- d. Between in and around March 2021 to December 2023, Garantex processed at least approximately \$1.2 million from, and to, three different darknet markets that specialized in drug sales and child sexual abuse material.

13. BESCIOKOV and MIRA SERDA knew that criminal proceeds were being laundered through Garantex. For example, between on or about June 17, 2019, through at least in and around March 2024, MIRA SERDA operated another exchange—CryptoMax—that facilitated anonymous illicit transactions through an account at Garantex registered to MIRA SERDA. CryptoMax publicly advertised that it offered parties instant, anonymous, exchanges or conversions between different types of cryptocurrencies, without the need to register an account. Using Garantex’s infrastructure, CryptoMax processed transactions to numerous illicit exchanges, including sending funds to darknet drug markets and other cryptocurrency laundering services. Additionally, via internal communications, BESCIOKOV identified CryptoMax transactions as Garantex processing “dirty funds.” However, neither he nor others blocked the CryptoMax account. To the contrary, the CryptoMax account was internally described as a “Trusted Exchanger” and “Our Exchanger,” and the account received tens of millions of dollars.

14. Moreover, Garantex administrators shielded MIRA SERDA’s identity from Russian law enforcement. Garantex administrators provided incomplete information in response to requests for information from Russian authorities about transactions processed by MIRA SERDA’s CryptoMax account and falsely claimed the account was not verified when, in fact, Garantex had associated the account with MIRA SERDA’s personal identifying documents.

15. Furthermore, BESCIOKOV personally identified, but nonetheless allowed, numerous other transactions and accounts linked to cybercriminals and other illicit actors. For example, in December 2022, he identified two different accounts he believed to be transferring funds originating from the Lazarus Group, a group of North Korean cyber threat actors believed to be run by the North Korean government and that was sanctioned by OFAC in September 2019. The accounts continued transacting on Garantex through April and July 2023, respectively. BESCIOKOV likewise notated on or about May 20, 2023, that another account was receiving dirty funds, but the account was nonetheless allowed to continue operating on Garantex until at least November 2023.

16. Garantex administrators, including BESCIOKOV and MIRA SERDA, often collected little to no information about Garantex customers. Many individuals were thus allowed to transact on Garantex without having provided or verified basic information about their identities, locations, businesses, or the purposes of their transactions. For example, some accounts on Garantex were registered to customers using the names “Drug,” “hacker,” “taliban,” “Cashout,” “cleancoins,” and “God” and included no real information about the users behind the accounts.

17. At various times from in and around March 2019 to in and around April 2022, and then again from in and around June 2023 to March 2024, Garantex administrators employed Companies A, B, and C to provide blockchain analytics services to identify suspicious transactions. However, from in and around April 2022 to in and around June 2023, Garantex administrators used no blockchain analytics services at all.

18. Even when the blockchain analytics services identified illicit transactions, including transactions sent to and from known cybercrime and narcotics trafficking forums, Garantex administrators, including BESCIOKOV and MIRA SERDA, did not act. Instead,

Garantex administrators processed numerous flagged transactions and permitted the accounts to continue operating. For example:

- a. From on or about May 16, 2019, to April 6, 2022, Company A flagged approximately 15,000 incoming deposits to Garantex as having a risk score of 1.000—the highest possible risk score. Of those highest risk transactions, only 247 (or 1.6%) were marked as “rejected,” seven were notated as “suspected,” and eleven were marked as “fraudulent”; the remaining 98% of these highest risk transactions were marked as “accepted.”
- b. Between in and around June 2023 and November 2023, Company B flagged 20 deposits as “terrorism_financing,” but Garantex administrators processed the transactions anyway.
- c. In and around October 2022, a Garantex user admitted to Garantex administrators that the Garantex user’s account was likely involved in laundering the proceeds of narcotics transactions. Garantex administrators allowed the user to continue transacting on the platform through at least November 2023.

19. Even during the periods that Garantex used a blockchain analytics service, it did not screen for all criminal transactions. For example, from its launch in 2019 to approximately April 2022, Garantex did not screen for transactions involving child exploitation, sanctions violations, or terrorism financing.

(All in violation of Title 18, United States Code, Section 1956(h).)

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

THE GRAND JURY FURTHER CHARGES THAT:

20. The allegations in paragraphs 1 through 9 are incorporated by reference herein.

21. The International Emergency Economic Powers Act (“IEEPA”), codified at Title 50, United States Code, Sections 1701 to 1708, confers upon the President authority to deal with unusual and extraordinary threats to the national security and foreign policy of the United States. 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 title.” 50 U.S.C. § 1705(a).

22. Pursuant to IEEPA, the President issued Executive Order 14024 on April 15, 2021, finding that specified harmful foreign activities of the Russian government, including engaging in and facilitating malicious cyber-enabled activities against the United States and its allies and partners, constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States. Executive Order 14024 blocks all property and interests in property in the United States or within the possession or control of any U.S. person of any person designated pursuant to Executive Order 14024 and provides that such property and interests in such property may not be transferred, paid, exported, withdrawn, or otherwise dealt in. Executive Order 14024 further prohibits (a) the making of any contribution or provision of funds, goods, or services by, to, or for the benefit of any such designated person; (b) the receipt of any contribution or provision of funds, goods, or services from any such person; and (c) any 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 the Executive Order.

23. To implement Executive Order 14024, OFAC issued the Russian Harmful Foreign Activities Sanctions Regulations, 31 C.F.R. Part 587. These regulations incorporate by reference the prohibited transactions set forth in Executive Order 14024. *See* 31 C.F.R. § 587.201. The regulations also provide that the names of persons designated pursuant to Executive Order 14024 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. *See id.* Note 1.

24. From on or about April 6, 2022, and continuing to the present, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendant, ALEKSEJ BESCIOKOV, did knowingly and willfully combine, conspire, confederate, and agree with others known and unknown to the Grand Jury to violate, and to cause a violation of, licenses, orders, regulations, and prohibitions issued under IEEPA, in violation of Title 50, United States Code, Section 1705(a), Executive Order 14024, and 31 C.F.R. § 587.201.

25. It was a part and an object of the conspiracy that the defendant, ALEKSEJ BESCIOKOV, and others known and unknown, would and did cause U.S. persons to engage in transactions and dealings in property and interests in property of Garantex, whose property and interests in property were blocked pursuant to Executive Order 14024, including through the provision of funds, goods, and services to and for the benefit of Garantex and the receipt of funds, goods, and services from Garantex, without first obtaining the required approval of OFAC; and would and did engage in transactions that evaded, and had the purpose of evading, the prohibitions set forth in Executive Order 14024, in violation of Title 50, United States Code, Section 1705(a) and (c).

Sanctions Violations Allegations

It was part of the conspiracy that:

26. Garantex administrators, including BESCIOKOV, knew that OFAC had added Garantex to the SDN List. For example, on or about April 6, 2022, BESCIOKOV emailed a virtual server provider and told the provider that Garantex had been added by OFAC to its SDN List and stated that he could no longer use U.S. server providers. On or about April 8, 2022, Garantex administrators sent a mass email to Garantex customers specifically noting that OFAC had sanctioned Garantex.

27. Despite the fact that OFAC had sanctioned Garantex, from on or about April 6, 2022, and continuing through the present, BESCIOKOV rented servers for Garantex's use and benefit from a U.S.-based server provider. On various dates, including on or about May 1, 2022, BESCIOKOV used a U.S.-based payment processing company to transmit payment on behalf of Garantex to the U.S.-based server provider.

28. From on or about April 12, 2022, and continuing through the present, Garantex used a U.S.-based video sharing website to advertise and promote its services, including by providing instructional videos to customers. These instructions included guidance on how to use Garantex without having transactions blocked by other exchanges due to sanctions restrictions. For example, on or about July 10, 2023, Garantex administrators posted a video on the U.S.-based video sharing website explaining how to execute transactions between Garantex and a virtual currency exchange ("VCE-1") that has transaction-monitoring software that would otherwise allow VCE-1 to block transactions with Garantex. The video recommended using third-party platforms as intermediaries to ensure the safety of the transfer. When a viewer asked why funds

could not be transferred directly to VCE-1, the speaker responded (as translated from Russian), “Because Garantex is a sanctioned exchange.”

29. Beginning in and around early 2023, Garantex changed its system for managing its operational wallet infrastructure to prevent virtual currency exchanges, including U.S.-based exchanges, from detecting that they were transacting with Garantex. Specifically, starting in and around early 2023, instead of storing its funds in the same wallets for extended periods of time, Garantex administrators moved the exchange’s operational wallets storing USDT to new virtual currency addresses on a daily basis. By changing virtual currency addresses on a daily basis, Garantex was able to evade detection by blockchain analytics services that identify and would allow exchanges to block transactions with known Garantex addresses.

30. Consistent with the change to its operating wallet infrastructure, a Garantex administrator explained in a Russian-language posting on Telegram on or about December 10, 2023:

Tether only blocks wallets included in the OFAC 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

31. As a result of these and other evasion and concealment techniques, between on or about April 6, 2022, and on or about May 16, 2024, Garantex facilitated over 5,470 transactions worth over \$83 million with just one U.S.-based exchange (“VCE-2”) on the Tron and Ethereum networks. Between on or about April 6, 2022, and in and around March 2024, Garantex also facilitated approximately 3,700 transactions with another U.S.-based exchange (“VCE-3”), totaling approximately \$5.5 million on the Bitcoin network.

(All in violation of Title 50, United States Code, Section 1705(a) and (c).)

COUNT THREE

(Conspiracy to Operate an Unlicensed Money Transmitting
Business)

THE GRAND JURY FURTHER CHARGES THAT:

32. The allegations in paragraphs 1 through 9 are incorporated by reference herein.

33. From in and around June 2019 and continuing through the present, in an offense begun outside the jurisdiction of any particular State or district of the United States, and continued in the Eastern District of Virginia and elsewhere, the defendant, ALEKSEJ BESCIOKOV, did knowingly and intentionally combine, conspire, confederate, and agree with others known and unknown to the Grand Jury to violate Title 18, United States Code, Section 1960(b)(1)(B) and (b)(1)(C) by operating an unlicensed money transmitting business, that is, while failing to comply with the money transmitting business registration requirements under Title 31, United States Code, Section 5330 and regulations prescribed under such section, and otherwise involving the transportation and transmission of funds that defendant ALEKSEJ BESCIOKOV, and others known and unknown to the Grand Jury, knew to have been derived from a criminal offense and intended to be used to promote and support unlawful activity.

Overt Acts

34. In furtherance of the offenses which were the object of the conspiracy, between in and around March 2019 and in and around March 2024, Garantex conducted at least tens of thousands of cryptocurrency transactions with U.S.-based exchanges, including 16,600 transactions in bitcoin alone with VCE-3.

35. The acts specified in paragraphs 27 through 29 and paragraph 31 were also committed in furtherance of the offenses which were the object of the conspiracy alleged in the instant count and are incorporated here.

(All in violation of Title 18, United States Code, Section 371.)

NOTICE OF FORFEITURE

THE GRAND JURY FURTHER FINDS PROBABLE CAUSE THAT:

Pursuant to Federal Rule of Criminal Procedure 32.2(a), the defendants are hereby notified that, if convicted of any of the offenses alleged in Counts 1 and 3 of the Indictment, the defendants shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1), any property, real or personal, involved in the offense, or any property traceable to such property.

Pursuant to Federal Rule of Criminal Procedure 32.2(a), the defendants are hereby notified that if convicted of the offense alleged in Count 2 of the Indictment, the defendants shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1)(C) and 28 U.S.C. § 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to the offense.

[This space intentionally left blank.]

Pursuant to Title 21, U.S. Code, Section 853(p), the defendants shall forfeit substitute property, if, by any act or omission of the defendants, the property referenced above cannot be located upon the exercise of due diligence, has been transferred, sold to, or deposited with a third party; has been placed beyond the jurisdiction of the Court; has been substantially diminished in value; or has been commingled with other property which cannot be divided without difficulty.


(All in accordance with Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(1); Title 28, United States Code, Section 2461(c); Title 21 United States Code, Section 853; and Fed. R. Crim. P. 32.2.)

A TRUE BILL:

Pursuant to the E-Government Act,
The original of this page has been filed
under seal in the Clerk's Office

For person of the Grand Jury

Erik S. Siebert
United States Attorney



Zoe Bedell
Assistant United States Attorney

Tamara Livshiz
Trial Attorney, Computer Crime and Intellectual Property Section