ORIGINAL

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

United States of America

v.

Roman Vitalyevich Ostapenko, Alexander Evgenievich Oleynik, and Anton Vyachlavovich Tarasov

Criminal Indictment

No. 1:25-CR-001

The Grand Jury charges that:

Background

1. "Virtual currencies" are digital representations of value that, like traditional coin and paper currency, function as a medium of exchange (i.e., they can be digitally traded or transferred, and can be used for payment or investment purposes). Virtual currencies are a type of digital asset separate and distinct from digital representations of traditional currencies, securities, and other traditional financial assets. The exchange value of a particular virtual currency generally is based on agreement or trust among its community of users. Some virtual currencies have equivalent values in real currency or can act as a substitute for real currency, while others are specific to particular virtual domains (e.g., online gaming communities) and generally cannot be exchanged for real currency. Cryptocurrencies, like Bitcoin and Ether, are types of virtual

currencies, which rely on cryptography for security. Cryptocurrencies typically lack a central administrator to issue the currency and maintain payment ledgers. Instead, cryptocurrencies use 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.

2. A "blockchain" is a digital ledger run by a decentralized network of computers referred to as "nodes." Each node runs software that maintains an immutable and historical record of every transaction utilizing that blockchain's technology. Many digital assets, including virtual currencies, publicly record all of their transactions on a blockchain, including all of the known balances for each virtual currency address on the blockchain. Blockchains consist of blocks of cryptographically signed transactions, and blocks are added to the previous block after validation and after undergoing a consensus decision to expose and resist tampering or manipulation of the data. There are many different blockchains used by many different virtual currencies. For example, Bitcoin in its native state exists on the Bitcoin blockchain, while Ether exists in its native state on the Ethereum network.

3. A "virtual currency address" is an alphanumeric string that designates the virtual location on a blockchain where virtual currency can be sent and received.

4. "Bitcoin" is a type of virtual currency. Unlike traditional, government-controlled currencies (i.e., fiat currencies), such as the U.S.

dollar, Bitcoin is not managed or distributed by a centralized bank or entity. Because of that, Bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved and verified by computers running Bitcoin's software. Those computers are called nodes and there are such nodes all over the world, including in the Northern District of Georgia. Each node uses cryptography to record every Bitcoin transaction on the Bitcoin blockchain. The Bitcoin blockchain is a public, distributed ledger. Bitcoin can be exchanged for fiat currency, other virtual currencies, products, and services.

5. A "virtual currency mixing service," also known as a "mixer," is a service that allows users, for a fee, to send virtual currency to designated recipients in a manner designed to conceal and obfuscate the source of the virtual currency.

6. "The Onion Router," also known as "Tor," is free and open-source software for enabling anonymous communication. It directs internet traffic via a free, worldwide, volunteer overlay network that consists of more than seven thousand relays. Using Tor makes it more difficult to trace a user's internet activity.

7. "Ransomware" is a type of malware that allows cybercriminals to encrypt some or all of the data stored on a victim's computer and transmit some or all of the victim's data to another computer under the cybercriminals' control. After ransomware is deployed on a victim's computer, cybercriminals typically demand a ransom payment from the

victim in exchange for decrypting the victim's data and allegedly deleting or refraining from publishing a copy of the victim's stolen data.

Count One
Money Laundering Conspiracy

8. The Grand Jury re-alleges and incorporates by reference the factual allegations contained in paragraphs 1 through 7 of this Indictment as if fully set forth herein.

9. Beginning on or about October 18, 2018, and continuing until on or about November 27, 2023, in the Northern District of Georgia and elsewhere, the defendants, ROMAN VITALYEVICH OSTAPENKO, ALEXANDER EVGENIEVICH OLEYNIK, and ANTON VYACHLAVOVICH TARASOV, did knowingly combine, conspire, confederate, agree, and have a tacit understanding with each other and others unknown to the Grand Jury to commit an offense against the United States in violation of Title 18, United States Code, Section 1956, that is: to knowingly conduct and attempt to conduct financial transactions in and affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity – that is, wire fraud, in violation of Title 18, United States Code, Section 1343, illegal transactions with an access device, in violation of Title 18, United States Code, Section 1029(a)(5), intentional damage to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A), and extortion by threatening to obtain information from a protected computer and by demanding

money and other thing of value in relation to damage to a protected computer, in violation of Title 18, United States Code, Sections 1030(a)(7)(B) and (a)(7)(C)—knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(l)(B)(i).

Manner and Means

10. The defendants, ROMAN VITALYEVICH OSTAPENKO, ALEXANDER EVGENIEVICH OLEYNIK, and ANTON VYACHLAVOVICH TARASOV, and others unknown to the Grand Jury, operated, promoted, and used Blender.io and Sinbad.io, virtual currency mixing services for Bitcoin on the internet, to launder funds obtained through ransomware, virtual currency thefts, and other crimes. Blender.io and Sinbad.io were accessible to users across the world, including users located in the Northern District of Georgia, via the internet.

11. From on or about October 18, 2018, and continuing until in or about April 2022, Blender.io allowed a user, through visiting its website, to send Bitcoin to Blender.io to mix the Bitcoin with other Bitcoin from other users to conceal and disguise the nature, location, source, ownership, and control of the Bitcoin. To accomplish this, Blender.io would hold the Bitcoin sent by the user for a period of time designated by the user and

then send the same amount of Bitcoin—but obtained from other users' transfers to the mixer—minus a fee, to new virtual currency addresses for the user to receive the virtual currency. The time between transfers, the ratio of the amount transferred to each destination virtual currency address, and the number of destination virtual currency addresses served to conceal and disguise the connection between the source and destination virtual currency addresses.

12. Blender.io was advertised on internet forums, including Bitcointalk.org and Bits.media. The advertisements described the mixer, explained how to use it, and provided updates on the mixer's status. For example, on or about October 18, 2018, a post to Bitcointalk.org posted by "blenderio" described Blender.io's service, including three websites—two clearnet websites (a website that can be freely accessed through the public internet) and one Tor website. The post stated that Blender.io had a "No Logs Policy" and explained that "[t]here's absolutely no log whatsoever, and whatever trace does exist of your transaction is deleted as soon as your transaction goes through." The post also explained that no registration was required for users: "Blender.io doesn't require you to signup, register or provide any kind of detail except the receiving address! As there are no personal details asked for, there's no way your identity is compromised, or can be linked back to, because as far as blender.io goes they don't know who you are."

13. In furtherance of the conspiracy, on or about November 2, 2021, a transfer was conducted of approximately 0.385 Bitcoin (approximately $24,000 at the time of transfer) from a virtual currency address beginning with 34toMfv4 to Blender.io virtual currency addresses beginning with 3Er19fau and 3JLxpo96, which involved the proceeds of a specified unlawful activity, that is, intentional damage to a protected computer, in violation of Title 18, United States Code, Section 1030(a)(5)(A), and extortion by threatening to obtain information from a protected computer and by demanding money and other thing of value in relation to damage to a protected computer, in violation of Title 18, United States Code, Sections 1030(a)(7)(B) and (a)(7)(C), to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity.

14. On May 6, 2022, the Department of Treasury's Office of Foreign Assets Control ("OFAC") publicly sanctioned Blender.io, citing its use by the Democratic People's Republic of Korea to launder stolen virtual currency. OFAC's public sanctions announcement also explained that Blender.io laundered funds for multiple ransomware groups.

15. From on or about October 13, 2022, and continuing until on or about November 27, 2023, Sinbad.io allowed a user, through visiting its website, to send Bitcoin to Sinbad.io to mix the Bitcoin with other Bitcoin from other users to conceal and disguise the nature, location, source, ownership, and control of the Bitcoin. To accomplish this, Sinbad.io would hold the

Bitcoin sent by the user for a period of time designated by the user and then send the same amount of Bitcoin—but obtained from other users' transfers to the mixer—minus a fee, to new virtual currency addresses for the user to receive the virtual currency. The time between transfers, the ratio of the amount transferred to each destination virtual currency address, and the number of destination virtual currency addresses served to conceal and disguise the connection between the source and destination virtual currency addresses.

16. The Sinbad.io website contained a FAQ (Frequently Asked Questions) page that describes the mixer as "a service that obfuscates your bitcoin transactions. It takes your bitcoins and sends you back the ones from the pool, which are premixed and not connected with you. Thus it breaks the link between the transactions before and after the mixing and makes it impossible to track the connection between the bitcoins that came into the mixer and went out."

17. Sinbad.io's services were advertised on internet forums, including Bitcointalk.org. For example, on or about October 13, 2022, a post to Bitcointalk.org posted by "SinBad.io" described Sinbad.io as "secure, fast and easy to use." The post provided an update on the operation of Sinbad.io, explaining that "[t]he website design has been updated." The post also noted a change in "service address" and included links to the clearnet and Tor websites for the mixer.

18. In furtherance of the conspiracy, on or about June 4, 2023, a transfer was conducted of approximately 5.409 Bitcoin (approximately $147,136 at the time of transfer) from a virtual currency address beginning with bc1q84vp to Sinbad.io virtual currency addresses beginning with bc1qz8q3, bc1qny83, bc1qhr46, and bc1qwm0, which involved the proceeds of a specified unlawful activity, that is, wire fraud, in violation of Title 18, United States Code, Section 1343, and illegal transactions with an access device, in violation of Title 18, United States Code, Section 1029(a)(5), to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity.

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

Count Two
Operating Unlicensed Money Transmitting Business

19. The Grand Jury re-alleges and incorporates by reference the factual allegations contained in paragraphs 1 through 7 and 10 through 18 of this Indictment as if fully set forth herein.

20. Beginning on or about October 18, 2018, and continuing until in or about April 2022, in the Northern District of Georgia and elsewhere, the defendants, ROMAN VITALYEVICH OSTAPENKO, ALEXANDER EVGENIEVICH OLEYNIK, and ANTON VYACHLAVOVICH TARASOV, aided and abetted by each other and others unknown to the Grand Jury, knowingly conducted, controlled, managed, supervised, directed, and owned all and part of an unlicensed money transmitting business affecting

interstate and foreign commerce, to wit, Blender.io, while failing 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 otherwise involving the transportation and transmission of funds that defendants OSTAPENKO, OLEYNIK, and TARASOV, and others 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, to wit, defendants OSTAPENKO, OLEYNIK, and TARASOV, and others unknown to the Grand Jury, used Blender.io to transmit millions of dollars by means of virtual currency transactions, including funds known to defendants OSTAPENKO, OLEYNIK, and TARASOV, and others unknown to the Grand Jury, to have been derived from a criminal offense and intended to be used to promote and support unlawful activity, without registering Blender.io as a money transmitting business under federal law, in violation of Title 18, United States Code, Section 1960 and Section 2.

Count Three
Operating Unlicensed Money Transmitting Business

21. The Grand Jury re-alleges and incorporates by reference the factual allegations contained in paragraphs 1 through 7 and 10 through 18 of this Indictment as if fully set forth herein.

22. Beginning on or about October 13, 2022, and continuing until on or about November 27, 2023, in the Northern District of Georgia and

elsewhere, the defendant, ROMAN VITALYEVICH OSTAPENKO, aided and abetted by others unknown to the Grand Jury, knowingly conducted, controlled, managed, supervised, directed, and owned all and part of an unlicensed money transmitting business affecting interstate and foreign commerce, to wit, Sinbad.io, while failing 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 otherwise involving the transportation and transmission of funds that defendant OSTAPENKO, and others 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, to wit, defendant OSTAPENKO, and others unknown to the Grand Jury, used Sinbad.io to transmit millions of dollars by means of virtual currency transactions, including funds known to defendant OSTAPENKO and others unknown to the Grand Jury to have been derived from a criminal offense and intended to be used to promote and support unlawful activity, without registering Sinbad.io as a money transmitting business under federal law, in violation of Title 18, United States Code, Section 1960 and Section 2.

Forfeiture

23. Upon conviction of one or more of the offenses alleged in Counts One through Three of this Indictment, the defendants, ROMAN VITALYEVICH OSTAPENKO, ALEXANDER EVGENIEVICH OLEYNIK, and ANTON VYACHLAVOVICH TARASOV, shall forfeit to the United States of America, pursuant to Title 18, United States Code, Section 982(a)(1), any property, real or personal, involved in such offense, and any property traceable to such property. The property to be forfeited includes, but is not limited to, the following:

> MONEY JUDGMENT: A sum of money in United States currency, representing the amount of proceeds obtained as a result of the offenses alleged in Counts One through Three of this Indictment.

24. If, as a result of any act or omission of the defendants, ROMAN VITALYEVICH OSTAPENKO, ALEXANDER EVGENIEVICH OLEYNIK, and ANTON VYACHLAVOVICH TARASOV, any property subject to forfeiture:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(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 divided without difficulty;

the United States intends, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b)(1), to seek forfeiture of any other property of said defendant up to the value of the forfeitable property.

A True BILL

FOREPERSON

RYAN K. BUCHANAN
United States Attorney

SAMIR KAUSHAL
Assistant United States Attorney
Georgia Bar No. 935285

ETHAN CANTOR
Trial Attorney, Computer Crime and Intellectual Property Section

600 U.S. Courthouse
75 Ted Turner Drive SW
Atlanta, GA 30303
404-581-6000; Fax: 404-581-6181