



# U.S. Department of **JUSTICE**

The Department of Justice is posting this court document as a courtesy to the public. An official copy of this court document can be obtained (irrespective of any markings that may indicate that the document was filed under seal or otherwise marked as not available for public dissemination) on the Public Access to Court Electronic Records website at <https://pacer.uscourts.gov>. In some cases, the Department may have edited the document to redact personally identifiable information (PII) such as addresses, phone numbers, bank account numbers, or similar information, and to make the document accessible under Section 508 of the Rehabilitation Act of 1973, which requires federal agencies to make electronic information accessible to people with disabilities.

**SEALED**

TMS/ASJZ: F#2020R00126  
ANW 10/28/24

**IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MARYLAND**

**UNITED STATES OF AMERICA**

v.

**ROMAN BEREZHNOY and  
EGOR NIKOLAEVICH GLEBOV,**

**Defendants.**

**CRIMINAL NO. TDC-23-459**

**(Conspiracy to Commit an Offense Against the United States, 18 U.S.C. § 371; Conspiracy to Commit Wire Fraud, 18 U.S.C. § 1349; Unauthorized Access to a Protected Computer, 18 U.S.C. § 1030(a)(2); Intentional Damage to a Protected Computer, 18 U.S.C. § 1030(a)(5)(A); Threatening to Impair the Confidentiality of Stolen Data, 18 U.S.C. § 1030 (a)(7)(B); Transmitting a Demand in Relation to Damage to a Protected Computer, 18 U.S.C. § 1030(a)(7)(C); Wire Fraud, 18 U.S.C. § 1343; Aiding and Abetting, 18 U.S.C. § 2; Forfeiture, 18 U.S.C. §§ 982, 1030(i), 21 U.S.C. § 853, and 28 U.S.C. § 2461(c))**

**SUPERSEDING INDICTMENT**

**COUNT ONE**

**(Conspiracy to Commit an Offense Against the United States)**

The Grand Jury for the District of Maryland charges that:

At all times relevant to this Superseding Indictment:

1. The defendants, **ROMAN BEREZHNOY** and **EGOR NIKOLAEVICH GLEBOV**, were Russian nationals residing outside the United States.

2. From at least in or around May 2019, and continuing through the date of this Superseding Indictment, **BEREZHNOY, GLEBOV**, and others conspired to operate as a cybercrime group using the Phobos ransomware, including through Phobos affiliate identifier “2803” and the name “8Base,” among others, and to engage in an international computer hacking and extortion scheme that victimized more than 1,000 public and private entities (collectively, the

“Victims”) in the United States and elsewhere, including in the District of Maryland, and to obtain ransom payments worth in excess of \$16 million dollars. Many of the Victims also suffered additional losses resulting from the loss of access to their data.

3. As part of the scheme, the co-conspirators hacked into the Victims’ computer networks, often using stolen or otherwise unauthorized credentials; copied and stole files and programs on the Victims’ networks; and encrypted the original versions of the stolen data on the Victims’ networks by installing and executing a form of malicious software known as “Phobos ransomware,” with the objective of preventing the Victims from accessing or using the data on the compromised networks. The co-conspirators then extorted the Victims for ransom payments in exchange for the decryption keys to regain access to the encrypted data by, among other things, leaving a ransom note on compromised Victim computers and calling and emailing Victims to initiate ransom payment negotiations. The co-conspirators also threatened to expose Victims’ stolen files to the public or to the Victims’ clients, customers, or constituents if the ransoms were not paid.

#### **Relevant Terms**

4. “Bitcoin” or “BTC” was a type of virtual currency that was circulated over the internet as a form of value. Bitcoin was not issued by any government, bank, or company, but rather, were generated and controlled through computer software operating via a decentralized, peer-to-peer network. Bitcoin was just one of many varieties of virtual currency.

5. A “darknet website” was a hidden website available through a network of globally distributed relay computers called the Tor network. Unlike typical websites on the internet, Tor-based websites anonymized internet activity by routing a user’s communications through the network of relay computers (or proxies), effectively masking information about the user’s computer.

6. “Encryption” was the translation of data into a secret code. In order to access encrypted data, a user had to have access to a password (known as a “decryption key”) that enabled the user to decrypt the data.

7. “Malware” was malicious computer software intended to cause the Victim computer to behave in a manner inconsistent with the intention of the owner or user of the Victim computer, usually unbeknownst to that owner or user.

8. “Phobos ransomware” was a form of sophisticated malware that infected a computer by targeting vulnerabilities in remote desktop protocol (“RDP”) and encrypted some or all of the data on the computer using file extensions such as “.devil,” “.devos,” “.help,” “.phobos,” and “.eight.” Once data on a computer was encrypted, distributors of the malware could then extort Victims by demanding a ransom in exchange for the decryption key needed to regain access to the encrypted data on the computer.

### The Conspiracy

9. Beginning no later than in or around May 2019, and continuing through the date of this Superseding Indictment, in the District of Maryland and elsewhere, the defendants, **ROMAN BEREZHNOY** and **EGOR NIKOLAEVICH GLEBOV**, did knowingly and unlawfully conspire with others known and unknown to the Grand Jury to commit an offense against the United States, that is:

a. to intentionally access a computer without authorization and thereby obtain information from any protected computer for the purpose of commercial advantage and private financial gain, in violation of Title 18, United States Code, Section 1030(a)(2) and (c)(2)(B)(i);

b. to knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer, with such offense causing: loss to 1 or more persons during a 1-year period

aggregating at least \$5,000 in value; the modification and impairment, and potential modification and impairment, of the medical examination, diagnosis, treatment, and care of 1 or more individuals; damage affecting a computer used by and for an entity of the United States Government in furtherance of the administration of justice, national defense, and national security; and damage affecting 10 or more protected computers during a 1-year period; in violation of Title 18, United States Code, Section 1030(a)(5)(A) and (c)(4)(B);

c. with intent to extort from a person money and other things of value, transmit in interstate and foreign commerce any communication containing a threat to obtain information from a protected computer without authorization and to impair the confidentiality of information obtained from a protected computer without authorization, in violation of Title 18, United States Code, Section 1030(a)(7)(B) and (c)(3)(A); and

d. with intent to extort from a person money and other things of value, transmit in interstate and foreign commerce any communication containing a demand and request for money and other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion, in violation of Title 18, United States Code, Section 1030(a)(7)(C) and (c)(3)(A).

#### **Objects of the Conspiracy**

10. The objects of the conspiracy involving **BEREZHNOY, GLEBOV**, and co-conspirators were to: (i) gain unauthorized access to Victims' computers; (ii) copy and steal data from Victims' computers; (iii) install and execute the Phobos ransomware on Victims' computers, resulting in the encryption of data on the computers; (iv) extort Victims by demanding a ransom paid in Bitcoin in exchange for decryption keys for the encrypted data; (v) threaten to release stolen data if the ransom was not paid; (vi) collect ransom payments from Victims that paid the ransom; and (vii) distribute ransom proceeds to **BEREZHNOY, GLEBOV**, and their co-conspirators.

**Manner and Means of the Conspiracy**

11. It was part of the conspiracy that the co-conspirators gained unauthorized access to computers within the Victims' networks and stole copies of data that could be accessed from the Victims' compromised computers. The co-conspirators often used credentials obtained through theft or other illicit means to gain access to the computers without authorization and sought out data that they deemed to be valuable or sensitive to the Victims.

12. It was further part of the conspiracy that the co-conspirators exploited their unauthorized access to Victim computer networks by installing and executing Phobos ransomware onto many of the Victims' computers, which caused the widespread encryption of data accessible to those computers. The co-conspirators deployed the ransomware for the purpose of making the data inaccessible to the Victims and thereby disrupting the Victims' business operations. The ransomware attacks caused the Victims to suffer substantial losses exceeding \$5,000, including from the damage caused to their computers and the disruptions to their businesses.

13. It was further part of the conspiracy that the co-conspirators left ransom notes on compromised Victim computers in the form of files. In the ransom notes, the co-conspirators typically notified each Victim that all their files had been encrypted and that they must pay a ransom in Bitcoin for decryption. The notes directed each Victim to contact the co-conspirators at specified email addresses to negotiate the ransom payment in exchange for the co-conspirators providing the Victims with the decryption keys needed to restore their access to encrypted data. The notes also instructed each Victim to include a specified alphanumeric string followed by "2803" in the subject line of any email. The co-conspirators often followed up with emails or

phone calls to the Victims in which the co-conspirators threatened to sell or otherwise expose the Victim's stolen data if the Victim refused to pay the ransom.

14. It was further part of the conspiracy that the co-conspirators established a Twitter account to broadcast their threats and to intimidate Victims.

15. It was further part of the conspiracy that the co-conspirators established a darknet website where: (a) they repeated their threats and (b) if a Victim did not pay the ransom, the co-conspirators published the stolen data.

16. It was further part of the conspiracy that the co-conspirators collected payments in Bitcoin from Victims that paid ransoms and distributed the proceeds amongst themselves. **BEREZHNOY** and **GLEBOV** frequently received payments from co-conspirators during the course of the conspiracy. Although the value of Bitcoin fluctuated, the co-conspirators successfully extorted various amounts of Bitcoin from Victims that, measured at the time the ransoms were paid, were worth millions of dollars.

#### Overt Acts

17. In furtherance of the conspiracy, and to effect the objects thereof, at least one of the co-conspirators performed and caused to be performed one of the following overt acts on or about the dates set forth below in the District of Maryland and elsewhere:

18. On or about February 2, 2020, **GLEBOV** accessed a particular online account for obtaining virtual phone numbers that the co-conspirators used to further Phobos ransomware activity.

19. On or about June 5, 2020, **GLEBOV** transferred 0.5 Bitcoin from a Phobos ransomware payment to a Bitcoin wallet address used by the co-conspirators to receive Phobos ransomware payments.

20. In or around April 2023, **BEREZHNOY** announced on a criminal internet forum

that he represented a “team” that was seeking to “buy access to corporate networks” through virtual private networks or RDP, and that the team was “looking for long-term suppliers, not a one-time sale.” **BEREZHNOY** stated that the target corporate networks should have revenue “of at least 5 million” and that the team was interested in networks located in the United States, the United Kingdom, Canada, Australia, Italy, France, and Germany. **BEREZHNOY** also stated that the team would be willing to work with others in exchange for a percent of the proceeds.

#### **Victim A**

21. In or around November 2020, one or more co-conspirators accessed the computer network of a Maryland-based company that provided accounting and consulting services to federal agencies (“Victim A”), deployed the Phobos ransomware on its computers, including computers located in the District of Maryland, and caused the encryption of Victim A’s data, all without Victim A’s permission.

22. At or around the same time, one or more co-conspirators transmitted a demand that Victim A pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

23. In or around February 2021, one or more co-conspirators provided Victim A with decryption keys in exchange for Victim A’s payment of a ransom in Bitcoin that was then equivalent to approximately \$12,000.

#### **Victim B**

24. In or around December 2021, one or more co-conspirators accessed the computer network of a Maryland-based managed services company (“Victim B”).

25. At or around the same time, the co-conspirators used a spreadsheet file—that was saved in an online account created by **BEREZHNOY** to keep track of user credentials and other information relating to Victim B’s network.

26. At or around the same time, one or more co-conspirators deployed the Phobos



ransomware on Victim B's computers, including computers located in the District of Maryland, and caused the encryption of Victim B's data, all without Victim B's permission.

27. At or around the same time, one or more co-conspirators transmitted a demand that Victim B pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

28. At or around the same time, one or more co-conspirators transmitted a threat to publish or otherwise expose data stolen from Victim B's computers if Victim B did not pay the ransom.

### **Victim C**

29. In or around July 2022, one or more co-conspirators accessed the computer network of a Maryland-based healthcare provider ("Victim C"), deployed the Phobos ransomware on its computers, including computers located in the District of Maryland, and caused the encryption of Victim C's data, all without Victim C's permission.

30. At or around the same time, one or more co-conspirators transmitted a demand that Victim C pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

31. At or around the same time, one or more co-conspirators provided Victim C with decryption keys in exchange for Victim C's payment of a ransom in Bitcoin that was then equivalent to approximately \$25,000.

### **Victim D**

32. In or around August 2022, one or more co-conspirators accessed the computer network of another Maryland-based healthcare provider ("Victim D"), deployed the Phobos ransomware on its computers, including computers in the District of Maryland, and caused the encryption of Victim D's data, all without Victim D's permission.

33. At or around the same time, one or more co-conspirators transmitted a demand that Victim D pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

34. At or around the same time, one or more co-conspirators transmitted a threat to publicly publish or otherwise expose data stolen from Victim D's computers if Victim D did not pay the ransom.

35. At or around the same time, one or more co-conspirators provided Victim D with decryption keys in exchange for Victim D's payment of a ransom in Bitcoin that was then equivalent to approximately \$37,000.

**Victim E**

36. In or around July 2023, one or more co-conspirators accessed the computer network of a Maryland-based law firm ("Victim E"), including computers in the District of Maryland, and stole data, all without Victim E's permission.

37. In or around July and August 2023, one or more co-conspirators transmitted a threat to publish or otherwise expose data stolen from Victim E's computers if Victim E did not pay a ransom.

**Victim F**

38. In or around April 2022, one or more co-conspirators accessed the computer network of a Pennsylvania-based healthcare company ("Victim F"), deployed ransomware on its computers, and caused the encryption of Victim F's data, all without Victim F's permission.

39. At or around the same time, one or more co-conspirators transmitted a demand that Victim F pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

40. At or around the same time, one or more co-conspirators provided Victim F with decryption keys in exchange for Victim F's payment of a ransom in Bitcoin that was then equivalent to approximately \$20,000.

**Victim G**

41. In or around May 2022, one or more co-conspirators accessed the computer network of an Arizona-based marketing and data analytics firm (“Victim G”), deployed ransomware on its computers, and caused the encryption of Victim G’s data, all without Victim G’s permission.

42. At or around the same time, one or more co-conspirators transmitted a demand that Victim G pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

43. At or around the same time, one or more co-conspirators provided Victim G with decryption keys in exchange for Victim G’s payment of a ransom in Bitcoin that was then equivalent to approximately \$40,000.

**Victim H**

44. In or around July 2022, one or more co-conspirators accessed the computer network of a New York-based law enforcement union (“Victim H”), deployed the Phobos ransomware on its computers, and caused the encryption of Victim H’s data, all without Victim H’s permission.

45. At or around the same time, one or more co-conspirators transmitted a demand that Victim H pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

46. At around the same time, one or more co-conspirators transmitted a threat to publish or otherwise expose data stolen from Victim H’s computers if Victim H did not pay the ransom.

**Victim I**

47. In or around July 2022, one or more co-conspirators accessed the computer network of a federally recognized tribe (“Victim I”), deployed the Phobos ransomware on its computers, and caused the encryption of Victim I’s data, all without Victim I’s permission.

48. At or around the same time, one or more co-conspirators transmitted a demand that Victim I pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

**Victim J**

49. In or around July 2023, one or more co-conspirators accessed the computer network of a Connecticut-based public school system (“Victim J”), deployed ransomware on its computers, and caused the encryption of Victim J’s data, all without Victim J’s permission.

50. At or around the same time, one or more co-conspirators transmitted a demand that Victim J pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

51. At around the same time, one or more co-conspirators transmitted a threat to publish or otherwise expose data stolen from Victim J’s computers if Victim J did not pay the ransom.

**Victim K**

52. In or around August 2022, one or more co-conspirators accessed the computer network of an Illinois-based contractor for the U.S. Department of Defense and the U.S. Department of Energy (“Victim K”), deployed the Phobos ransomware on its computers, and caused the encryption of Victim K’s data, all without Victim K’s permission.

53. At or around the same time, one or more co-conspirators transmitted a demand that Victim K pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

**Victim L**

54. In or around May 2023, one or more co-conspirators accessed the computer network of an Ohio-based automotive company (“Victim L”), deployed the Phobos ransomware on its computers, and caused the encryption of Victim L’s data, all without Victim L’s permission.

55. In or around May and June 2023, one or more co-conspirators transmitted a demand that Victim L pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

56. At around the same time, one or more co-conspirators transmitted a threat to publish or otherwise expose data stolen from Victim L's computers if Victim L did not pay the ransom.

**Victim M**

57. In or around June 2023, one or more co-conspirators accessed the computer network of a California-based public school system ("Victim M"), deployed the Phobos ransomware on its computers, and caused the encryption of Victim M's data, all without Victim M's permission.

58. At or around the same time, one or more co-conspirators transmitted a demand that Victim M pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

59. At or around the same time, one or more co-conspirators transmitted a threat to publish or otherwise expose data stolen from Victim M's computers if Victim M did not pay the ransom.

60. At or around the same time, one or more co-conspirators provided Victim M with decryption keys in exchange for Victim M's payment of a ransom in Bitcoin that was then equivalent to approximately \$300,000.

**Victim N**

61. In or around September 2023, one or more co-conspirators accessed the computer network of a North Carolina-based children's hospital ("Victim N"), deployed the Phobos ransomware on its computers, and caused the encryption of Victim N's data, all without Victim N's permission.

62. At or around the same time, one or more co-conspirators transmitted a demand that Victim N pay a ransom in Bitcoin in exchange for decryption keys for the encrypted data.

63. At or around the same time, one or more co-conspirators transmitted a threat to publish or otherwise expose data stolen from Victim N's computers if Victim N did not pay the ransom.

64. At or around the same time, one or more co-conspirators provided Victim N with decryption keys in exchange for Victim N's payment of a ransom in Bitcoin that was then equivalent to approximately \$100,000.

18 U.S.C. § 371

**COUNT TWO**  
**(Wire Fraud Conspiracy)**

1. The allegations contained in Paragraphs 1 through 8 and Paragraphs 11 through 64 of Count One of this Superseding Indictment are re-alleged and incorporated as though fully set forth herein.

2. Beginning no later than in or around May 2019, and continuing through the date of this Superseding Indictment, in the District of Maryland and elsewhere, the defendants, **ROMAN BEREZHNOY** and **EGOR NIKOLAEVICH GLEBOV**, did knowingly and unlawfully conspire and agree with others, known and unknown to the Grand Jury, to devise a scheme and artifice to defraud, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises—to wit, to use access credentials without authorization to remotely access Victims' networks in order to encrypt Victims files for the purpose of extorting ransom payments—and to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce certain writings, signs, signals, and sounds in furtherance of such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

18 U.S.C. § 1349

**COUNTS THREE THROUGH FIVE**  
**(Intentional Damage to a Protected Computer)**

1. The allegations contained in Paragraphs 1 through 8 and Paragraphs 11 through 64 of Count One of this Superseding Indictment are re-alleged and incorporated as though fully set forth herein.

2. On or about the dates identified below, in the District of Maryland and elsewhere, the defendants, **ROMAN BEREZHNOY** and **EGOR NIKOLAEVICH GLEBOV**, did knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage without authorization to a protected computer; and the offense caused: loss to 1 or more persons during a 1-year period aggregating at least \$5,000 in value; the modification and impairment, and potential modification and impairment, of the medical examination, diagnosis, treatment, and care of 1 or more individuals; and damage affecting 10 or more protected computers during a 1-year period.

<b>COUNT</b>	<b>DATE</b>	<b>VICTIM</b>
Three	On or about December 26, 2021	Victim B
Four	In or around July 2022	Victim C
Five	On or about August 10, 2022	Victim D

18 U.S.C. § 1030(a)(5)(A), (c)(4)(B)  
 18 U.S.C. § 2



**COUNTS SIX THROUGH EIGHT**  
**(Transmitting a Demand in Relation to Damage to a Protected Computer)**

1. The allegations contained in Paragraphs 1 through 8 and Paragraphs 11 through 64 of Count One of this Superseding Indictment are re-alleged and incorporated as though fully set forth herein.

2. On or about the dates identified below, in the District of Maryland and elsewhere, the defendants, **ROMAN BEREZHNOY** and **EGOR NIKOLAEVICH GLEBOV**, did, with intent to extort from a person money and other things of value, transmit in interstate and foreign commerce a communication containing a demand and request for money and other things of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion.

<b>COUNT</b>	<b>DATE</b>	<b>VICTIM</b>
Six	On or about December 28, 2021	Victim B
Seven	In or around July 2022	Victim C
Eight	On or about August 10, 2022	Victim D

18 U.S.C. § 1030(a)(7)(C), (c)(3)(A)  
 18 U.S.C. § 2

**COUNT NINE**

**(Unauthorized Access to a Protected Computer)**

1. The allegations contained in Paragraphs 1 through 8 and Paragraphs 11 through 64 of Count One of this Superseding Indictment are re-alleged and incorporated as though fully set forth herein.

2. In or around June 2023, in the District of Maryland and elsewhere, the defendants, **ROMAN BEREZHNOY** and **EGOR NIKOLAEVICH GLEBOV**, did intentionally access a computer used by Victim E without authorization and thereby obtain information from a protected computer, and such offense was committed for the purpose of private financial gain.

18 U.S.C. § 1030(a)(2)(C), (c)(2)(B)  
18 U.S.C. § 2

**COUNT TEN**

**(Transmitting Threat to Impair the Confidentiality of Stolen Data)**

1. The allegations contained in Paragraphs 1 through 8 and Paragraphs 11 through 64 of Count One of this Superseding Indictment are re-alleged and incorporated as though fully set forth herein.

2. In or around June 2023, in the District of Maryland and elsewhere, the defendants, **ROMAN BEREZHNOY** and **EGOR NIKOLAEVICH GLEBOV**, did, with intent to extort from a person money and other things of value, transmit in interstate and foreign commerce a communication containing a threat to impair the confidentiality of information obtained from a protected computer used by Victim E without authorization.

18 U.S.C. § 1030(a)(7)(B), (c)(3)(A)  
18 U.S.C. § 2

**COUNT ELEVEN**  
**(Wire Fraud)**

1. The allegations contained in Paragraphs 1 through 8 and Paragraphs 11 through 64 of Count One of this Superseding Indictment are re-alleged and incorporated as though fully set forth herein.

2. In or around December 2021, in the District of Maryland and elsewhere, the defendants, **ROMAN BEREZHNOY** and **EGOR NIKOLAEVICH GLEBOV**, did knowingly and intentionally devise a scheme and artifice to defraud Victim B, and to obtain money and property from Victim B by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate commerce and foreign commerce to Maryland, certain writings, signals, signs and sounds: to wit, for the purpose of executing and attempting to execute a scheme to use unauthorized access credentials to remotely access Victim B's network to encrypt Victim B's files in order to demand a ransom payment, **BEREZHNOY** and **GLEBOV** transmitted and caused to be transmitted an email from fulpori442@gmail to info@[Victim B].com in Maryland demanding payment to decrypt Victim B's data, which transmission was routed through a server located outside the State of Maryland.

18 U.S.C. § 1343  
18 U.S.C. § 2

**FORFEITURE ALLEGATION**

The Grand Jury for the District of Maryland further finds that:

1. Pursuant to the Federal Rule of Criminal Procedure 32.2, notice is hereby given to the defendants that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2)(B) and (b), and 1030(i); Title 21, United States Code, Section 853; and Title 28, United States Code, Section 2461(c), in the event of the defendant's conviction under Counts One through Eleven of this Superseding Indictment.

**Computer Fraud Forfeiture**

2. Upon conviction of the offenses set forth in Counts One, Three, Four, Five, Six, Seven, Eight, Nine, and Ten, the defendants,

**ROMAN BEREZHNOY, and  
EGOR NIKOLAEVICH GLEBOV,**

shall forfeit to the United States of America, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i) and Title 21, United States Code, Section 853, any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly, as a result of such offense, including but not limited to, a money judgment representing the proceeds of such offense; and pursuant to all right, title, and interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such offense.

**Wire Fraud Forfeiture**

3. Upon conviction of the offenses set forth in Counts Two and Eleven, the defendants,

**ROMAN BEREZHNOY, and  
EGOR NIKOLAEVICH GLEBOV,**

shall forfeit to the United States of America, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), any property, real or personal, which constitutes, or is derived from, proceeds traceable to such offense.


Substitute Assets

4. If any of the property described above, as a result of any act or omission of the defendant:

- a. cannot be located upon the exercise of due diligence;
- b. has been transferred, 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 shall be entitled to forfeiture of substitute property of the Defendants up to the value of the above-described forfeitable property, pursuant to Title 21, United States Code, 853(p), as incorporated by Title 18, United States Code, Section 982(b) and Title 28, United States Code, Section 2461(c).

18 U.S.C. § 981(a)(1)(C)  
18 U.S.C. § 982(a)(2)(B) and (b)  
18 U.S.C. § 1030(i)  
21 U.S.C. § 853  
28 U.S.C. § 2451(c)

  
Erek L. Barron  
United States Attorney

A TRUE BILL

**SIGNATURE REDACTED**

Foreperson 

Date: 10/31/2024