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

UNITED STATES OF AMERICA

v.

[redacted]

SERGEI ANATOLYEVICH FILIMONOV

Criminal Indictment

No. 1 25-CR-0491

UNDER SEAL

THE GRAND JURY CHARGES THAT:

Count One
(18 U.S.C. § 1349, Bank and Wire Fraud Conspiracy)

1. From at least in or about November 2023, and continuing through in or about October 2025, in the Northern District of Georgia and elsewhere, the defendants, [redacted] and SERGEI ANATOLYEVICH FILIMONOV, did knowingly and willfully combine, conspire, confederate, agree, and have a tacit understanding with each other and others known and unknown to the Grand Jury,

a. to knowingly execute and attempt to execute a scheme and artifice to defraud federally insured financial institutions, and to obtain moneys, funds, assets, and property owned by and under the custody and control of federally insured financial institutions, by means of materially false and fraudulent pretenses, representations,

and promises, in violation of Title 18, United States Code, Section 1344; and

b. to devise and intend 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, and by omission of material facts, well knowing and having reason to know that said pretenses were and would be false and fraudulent when made and caused to be made and that said omissions were and would be material, and, in so doing, to cause interstate and foreign wire communications to be made, in furtherance of the scheme and artifice to defraud, thereby affecting a financial institution, in violation of Title 18, United States Code, Section 1343.

Background

At all times relevant to this Indictment:

2. [redacted]

3. FILIMONOV was a Russian national located outside of the United States.

4. "Login credentials" were account access information, including a user identifier and password, assigned by financial institutions to individual customers. Financial institutions required their customers to input their login credentials on banking websites to authenticate those customers' identities before authorizing account access.

5. "Banking websites" were websites maintained by financial institutions to provide their customers with online access to authorized financial accounts, including the ability to send and receive wire transactions from those accounts.

6. A "spoofed domain" was a web domain created to imitate the domain of a legitimate company.

7. A "sponsored link" was a paid advertisement displayed by a search engine. Sponsored links can be purchased and appear when search engine users search for specific keywords.

8. COMPANY-1 was headquartered in Atlanta, Georgia, in the Northern District of Georgia. C.W. was employed by COMPANY-1.

9. COMPANY-2 maintained an office in Cumming, Georgia, in the Northern District of Georgia. S.C. was employed by COMPANY-2.

10. Aston Eric, LLC was a company registered with the Georgia Secretary of State on or about April 4, 2024. Aston Eric, LLC maintained an account ending in x0077 at BANK-2.

11. BANK-1 and BANK-2 were financial institutions federally insured by the Federal Deposit Insurance Corporation with headquarters in North Carolina and local branches within the Northern District of Georgia.

12. COMPANY-1 maintained bank accounts ending in x1681 and x0489 at a branch office of BANK-1 located in the Northern District of Georgia.

13. C.W. maintained login credentials assigned by BANK-1 that authorized C.W. to access COMPANY-1's accounts ending in x1681 and x0489 through BANK-1's banking website.

14. COMPANY-2 maintained bank accounts ending in x7343 and x8643 at a branch office of BANK-2 located in the Northern District of Georgia.

15. S.C. maintained login credentials assigned by BANK-2 that authorized S.C. to access COMPANY-2's accounts ending in x7343 and x8643 through BANK-2's banking website.

Manner and Means of Conspiracy

16. Beginning on a date unknown, but at least by in or about November 2023, and continuing through in or about October 2025, in the Northern District of Georgia and elsewhere, FILIMONOV and [redacted], and others known and unknown to the Grand Jury, carried out a scheme with the purpose of:

a. registering and maintaining spoofed domains of financial institutions;

b. purchasing sponsored links on search engines to direct individuals looking for their financial institution's banking website to spoofed domains imitating that financial institution;

c. stealing login credentials from victim bank customers who attempted to log into fraudulent websites hosted at the spoofed domains;

d. inducing customers to transmit other account security information, including answers to security questions or two-factor authentication text message codes;

e. creating and maintaining an interactive database of stolen login credentials, accessible to members of the conspiracy;

f. using stolen login credentials to log into banking websites without authorization;

g. using stolen login credentials to access banking websites and review account balances; and

h. using stolen login credentials to cause funds to be wired from the victims' accounts.

17. As a part of the conspiracy, [redacted] and others, using aliases, registered spoofed domains similar to the domains of BANK-1, BANK-2, and other financial institutions. These spoofed domains linked to webpages that appeared indistinguishable from the actual login pages of the financial institutions they sought to imitate.

18. FILIMONOV, [redacted], and others obtained sponsored links so that their spoofed domains would appear in search results when victims sought to access the banking website of their financial institution by searching for their financial institution using a search engine.

19. [redacted] and others purchased online infrastructure used in furtherance of the scheme, including websites, servers, and website traffic filtering tools.

20. FILIMONOV developed, tested, and maintained online infrastructure used in furtherance of the scheme, including the fraudulent websites imitating legitimate banking websites.

21. FILIMONOV, [redacted], and others created, developed, and maintained online infrastructure to store victim login credentials, transmit login credentials to co-conspirators, and track information about the compromised financial accounts to which the login credentials provided access.

22. In the course of the conspiracy, FILIMONOV, [redacted], and others collected and attempted to collect more than 5,000 victim login credentials to financial institutions, including BANK-1 and BANK-2. The victim login credentials included login credentials assigned to C.W. and S.C.

23. At times, to hinder detection of the unauthorized access to a victim's bank account, the conspirators sent hundreds of unsolicited emails to the email address associated with the victim's login credentials and bank account.

24. In the course of the conspiracy, the conspirators, using stolen victim login credentials, obtained and attempted to obtain millions of dollars from financial institutions, including from bank accounts belonging to COMPANY-1 and COMPANY-2.

25. It was further part of the conspiracy that FILIMONOV and [redacted] knowingly falsely registered domain names and knowingly used those domain names in the course of the offense, in violation of 18 U.S.C. § 3559(g)(1).

All in violation of Title 18, United States Code, Sections 1349 and 3559(g)(1).

Count Two
(18 U.S.C. § 1029(b)(2), Access Device Fraud Conspiracy)

26. The Grand Jury realleges and incorporates here the factual allegations in paragraphs 2 through 25 of this Indictment.

27. From at least in or about November 2023, and continuing through in or about October 2025, in the Northern District of Georgia and elsewhere, the defendants, [redacted] and SERGEI ANATOLYEVICH FILIMONOV, did knowingly and willfully combine, conspire, confederate, agree, and have a tacit understanding with each other and others known and unknown to the Grand Jury to commit the offense of access device fraud, to wit:

a. to knowingly and with intent to defraud, possess at least fifteen unauthorized access devices, namely, login credentials for banking websites of financial institutions, said possession affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(3);

b. to knowingly and with intent to defraud, possess device-making equipment, namely software designed to capture, transmit, and replicate, without authorization, login credentials for banking websites of financial institutions, said possession affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(4); and

c. to knowingly and with intent to defraud, effect transactions with at least one access device issued to another person to receive payment during a one-year period, the aggregate value of which is at least $1,000, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(5).

OVERT ACTS

28. In furtherance of the conspiracy, and to effect the objects thereof, the following overt acts, among others, were committed in the Northern District of Georgia and elsewhere:

29. On or about June 6, 2024, [redacted] and FILIMONOV stole online banking login credentials issued by BANK-1 assigned to C.W., an employee at COMPANY-1, through software code. The conspirators also induced C.W. to transmit additional information to bypass account security measures.

30. On or about June 7, 2024, one or more conspirators accessed COMPANY-1's accounts ending in x0489 and x1681 at BANK-1, located in the Northern District of Georgia, and caused and attempted to cause the unauthorized transfer of more than $5,000,000 from those accounts.

31. On or about November 15, 2024, [redacted] and FILIMONOV stole online banking login credentials issued by BANK-2 assigned to S.C., an employee at COMPANY-2, through software code. The conspirators also induced S.C. to transmit additional information to bypass account security measures.

32. On or about November 15, 2024, one or more conspirators accessed COMPANY-2's accounts ending in x7343 and x8643 at BANK-2, located in the Northern District of Georgia, and caused and attempted to cause the unauthorized transfer of approximately $735,000 from those accounts.

33. It was further part of the conspiracy that FILIMONOV and [redacted] knowingly falsely registered domain names and knowingly used those domain names in the course of the offense, in violation of 18 U.S.C. § 3559(g)(1).

All in violation of Title 18, United States Code, Sections 1029(b)(2) and 3559(g)(1).

Counts Three and Four
(18U.S.C. § 1344, Bank Fraud)

34. The Grand Jury realleges and incorporates here the factual allegations in paragraphs 2 through 25 and 28 through 33 of this Indictment.

35. From at least in or about November 2023 to in or about October 2025, in the Northern District of Georgia and elsewhere, the defendants, [redacted] and SERGEI ANATOLAVICH FILIMONOV, aided and abetted by each other and others known and unknown to the Grand Jury, did knowingly execute and attempt to execute a scheme and artifice described above in paragraphs 2 to 25, to defraud federally insured financial institutions, and to obtain moneys, funds, assets, and property owned by and under the

custody and control of federally insured financial institutions, by means of materially false and fraudulent pretenses, representations, and promises.

36. On or about each date listed below, in the Northern District of Georgia and elsewhere, for the purpose of executing the scheme and artifice to defraud and to obtain money from the federally insured financial institutions listed below, FILIMONOV and [redacted], aided and abetted by each other and others known and unknown to the Grand Jury, obtained and attempted to obtain by means of materially false pretenses, representations, and promises the following money owned by and under the custody and control of a financial institution at the accounts listed below:

Count	Date	Financial Institution	Victim	Account	Approximate Sum of Funds
3	6/7/2024	BANK-1	COMPANY-1	x0489 x1681	$5,579,800
4	11/15/2024	BANK-2	COMPANY-2	x7343 x8643	$735,000

All in violation of Title 18, United States Code, Sections 1344 and 2.

Counts Five and Six
(18 U.S.C. § 1343, Wire Fraud)

37. The Grand Jury realleges and incorporates here the factual allegations in paragraphs 2 through 25 and 28 through 33 of this Indictment.

38. On or about the dates set forth below, in the Northern District of Georgia and elsewhere, the defendants, [redacted] and SERGEI ANATOLYEVICH FILIMONOV, aided and abetted by each other and others

known and unknown to the Grand Jury, for the purpose of executing and attempting to execute the scheme and artifice described above in paragraphs 2 through 25, such scheme and artifice having been devised and intended to be devised to defraud, and for the purpose of obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, knowing and having reason to know that the pretenses, representations, and promises were and would be material, did, with the intent to defraud, cause the following wire communications to be transmitted in interstate and foreign commerce, affecting a financial institution:

Count	Date	Wire Communication
5	6/7/2024	Wire transfer of $299,600.00 from BANK-1 account ending in x0489, registered to COMPANY-1, to BANK-2 account ending in x0077, registered to Aston Eric LLC
6	11/22/2024	Electronic transmission of login credentials by S.C. to a server located outside of the United States

All in violation of Title 18, United States Code, Sections 1343 and 2.

Count Seven
(18 U.S.C. § 1029(a)(3), Possession of Unauthorized Access Devices)

39. The Grand Jury realleges and incorporates here the factual allegations in paragraphs 2 through 25 and 28 through 33 of this Indictment.

40. On or about October 6, 2025, outside of the United States, the defendants, [redacted] and SERGEI ANATOLYEVICH FILIMONOV,

who will be first brought to the Northern District of Georgia, aided and abetted by each other and others known and unknown to the Grand Jury, did knowingly and with intent to defraud possess at least fifteen unauthorized access devices, namely, approximately 5,000 login credentials for banking websites of financial institutions, including login credentials issued by BANK-1 for accessing COMPANY-1's accounts ending in x0489 and x1681 and by BANK-2 for accessing COMPANY-2's accounts ending in x7343 and x8643, that could be used alone and in conjunction with another access device to obtain money and other things of value, and could be used to initiate a transfer of funds, said possession affecting interstate and foreign commerce, all in violation of Title 18, United States Code, Sections 1029(a)(3), (c)(1)(A)(i), & (h), and 2.

Count Eight
(18 U.S.C. § 1029(a)(4), Possession of Device-Making Equipment)

41. The Grand Jury realleges and incorporates here the factual allegations in paragraphs 2 through 25 and 28 through 33 of this Indictment.

42. On or about October 6, 2025, outside of the United States, the defendants, [redacted] and SERGEI ANATOLYEVICH FILIMONOV, who will be first brought to the Northern District of Georgia, aided and abetted by each other and others known and unknown to the Grand Jury, did knowingly and with intent to defraud, possess device-making equipment, namely, software designed to capture, transmit, and replicate without authorization login

credentials for banking websites of financial institutions in the United States, including those associated with bank accounts located in the Northern District of Georgia, said possession affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 1029(a)(4), (c)(1)(A)(ii), & (h), and 2.

Count Nine
(18 U.S.C. § 1029(a)(5), Effecting Fraudulent Transactions with Access Devices)

43. The Grand Jury realleges and incorporates here the factual allegations in paragraphs 2 through 25 and 28 through 33 of this Indictment.

44. On or about June 7, 2024, in the Northern District of Georgia and elsewhere, the defendants, [redacted] and SERGEI ANATOLYEVICH FILIMONOV, aided and abetted by each other and others known and unknown to the Grand Jury, did knowingly and with intent to defraud, effect transactions with at least one access device issued to another person, including login credentials issued to C.W., to receive payment and any other thing of value, from on or about January 1, 2024 to January 1, 2025, the aggregate value of which is greater than $1,000, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 1029(a)(5), (c)(1)(A)(ii), & (h), and 2.

Counts Ten and Eleven
(18 U.S.C. § 1028A – Aggravated Identity Theft)

45. The Grand Jury realleges and incorporates here the factual allegations in paragraphs 2 through 25 and 28 through 33 of this Indictment.

46. On or about the dates set forth below, in the Northern District of Georgia, the defendants, [redacted] and SERGEI ANATOLYEVICH FILIMONOV, aided and abetted by each other and others known and unknown to the Grand Jury, did knowingly possess and use, without lawful authority, a means of identification of another person, as described below, during and in relation to felony violations of bank and wire fraud, conspiracy to commit bank and wire fraud, access device fraud conspiracy, and effecting fraudulent transactions with access devices:

Count	Date	Means of Identification
10	6/7/2024	Login Credentials of C.W. for BANK-1
11	11/15/2024	Login Credentials of S.C. for BANK-2

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

Forfeiture

47. Upon conviction of one or more of the offenses in Counts One through Nine of this Indictment, the defendants, SERGEI ANATOLYEVICH FILIMONOV and [redacted], shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 981(a)(1)(C), 982(a)(2), and Title 28, United States Code, Section 2461(c) any property, real or personal, which constitutes, or is derived from, proceeds traceable to the offenses, including, but 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 Nine of this Indictment.

48. If, as a result of any act or omission of the defendants, 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 subdivided without difficulty;

the United States of America intends, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), to

seek forfeiture of any other property of said defendants up to the value of the forfeitable property.

A TRUE BILL

FOREPERSON

THEODORE S. HERTZBERG
United States Attorney
/s/ Jessica C. Morris
JESSICA C. MORRIS
Assistant United States Attorney
Georgia Bar No. 1009078

/s/ Brian Z. Mund
BRIAN Z. MUND
Trial Attorney
California Bar No. 324699

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