

HIGHLY SENSITIVE DOCUMENT
UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

DOCKETED

HSD

UNITED STATES OF AMERICA

v.

VLADISLAV KLYUSHIN,
a/k/a "Vladislav Kliushin,"
IVAN ERMAKOV,
a/k/a "Ivan Yermakov," and
NIKOLAI RUMIANTCEV,
a/k/a "Nikolay Rummyantsev,"

Defendants

) 21-CR-10104

) Violations:

) Count One: Conspiracy to Obtain Unauthorized
) Access to Computers, and to Commit Wire
) Fraud and Securities Fraud
) (18 U.S.C. § 371)

) Count Two: Wire Fraud; Aiding and Abetting
) (18 U.S.C. §§ 1343 and 2)

) Count Three: Unauthorized Access to
) Computers; Aiding and Abetting
) (18 U.S.C. §§ 1030(a)(4) and 2)

) Count Four: Securities Fraud; Aiding and
) Abetting
) (15 U.S.C. §§ 78j(b) and 78ff(a); 17 C.F.R.
) § 240.10b-5; 18 U.S.C. § 2)

) Forfeiture Allegation:
) (18 U.S.C. §§ 981(a)(1)(C) and 28 U.S.C.
) § 2461(c))

) Computer Intrusion Forfeiture Allegation:
) 18 U.S.C. §§ 982(a)(2)(B) and 1030(i)

INDICTMENT

At all times relevant to this Indictment:

General Allegations

1. Defendant VLADISLAV KLYUSHIN, also known as "Vladislav Kliushin," was a Russian citizen who resided in Russia. KLYUSHIN was employed as the first deputy general

HIGHLY SENSITIVE DOCUMENT

director of M-13, a purported information technology company based in Moscow. At various times, KLYUSHIN purported to be the owner of M-13.

2. Defendant IVAN ERMAKOV, also known as “Ivan Yermakov,” was a Russian citizen who resided in Russia. ERMAKOV was employed as a deputy general director of M-13.

3. Defendant NIKOLAI RUMIANTCEV, also known as “Nikolay Rumyantsev,” was a Russian citizen who resided in Russia. RUMIANTCEV was employed as a deputy general director of M-13.

4. M-13 purported to offer information technology and media monitoring services, including monitoring and analytics of media and social media messages, cyber security consulting, and penetration testing. Penetration testing, also called pen testing, is an authorized, simulated cyberattack that is used to evaluate an organization’s ability to protect its computer systems, networks, and applications. A pen test looks for exploitable vulnerabilities in a computer system that could be leveraged by a hacker to obtain unauthorized access to the system.

5. According to M-13’s website, the company also provided “Advanced persistent threat (APT) Emulation” services that it described as the “most sound and modern method of testing and analyzing the infrastructure’s security.” The website explained: “Our experts imitate a full-scale targeted attack, during which the attacker, while trying to conceal his presence, uses a wide range of actions against the organization’s infrastructure.” The website further indicated that the company’s “IT solutions” were used by “the Administration of the President of the Russian Federation, the Government of the Russian Federation, federal ministries and departments, regional state executive bodies, commercial companies and public organizations.”

HIGHLY SENSITIVE DOCUMENT

6. KLYUSHIN, ERMAKOV and RUMLIANTCEV also purported to offer investment management services through M-13 to Individuals 1, 2 and 3, in exchange for up to 60 percent of the profits.

7. Filing Agent 1 and Filing Agent 2 were companies operating in the United States that, among other services, provided their clients with secure technology and communications platforms for preparing and submitting regulatory filings to the U.S. Securities and Exchange Commission (“SEC”). The clients of Filing Agent 1 and Filing Agent 2 were public companies, the securities of which were traded on national securities exchanges in the United States.

8. The New York Stock Exchange (the “NYSE”) and the NASDAQ Stock Market (the “NASDAQ”) were national securities exchanges in the United States.

9. The SEC was an independent agency of the executive branch of the United States government that was responsible for enforcing federal securities laws and promulgating rules and regulations thereunder.

10. Under United States securities laws, publicly traded companies must regularly disclose their financial performance to the SEC, and, through the SEC, to the general public. For example, publicly traded companies are generally required to file quarterly financial reports after each of the first three quarters of the fiscal year on SEC Form 10-Q, and to file an annual report of their financial performance, including audited financial statements, after the end of the final quarter of the fiscal year, on SEC Form 10-K. In addition, publicly traded companies are required to file periodic “current reports” (on SEC Form 8-K) disclosing events of significance to shareholders.

HIGHLY SENSITIVE DOCUMENT

11. Many reporting companies provide these financial reports to filing agents, such as Filing Agent 1 and Filing Agent 2, which file them electronically via the SEC's Electronic Data Gathering, Analysis and Retrieval system, commonly known as EDGAR. In order to make these EDGAR filings on behalf of their clients, filing agents first receive and store the companies' financial results on their own secure, internet-connected computer networks. Prior to their filing and public disclosure, the results are considered highly confidential business information.

Overview of the Conspiracy and the Scheme to Defraud

12. Beginning at least as early as January 2018 and continuing through at least September 2020, the defendants, KLYUSHIN, ERMAKOV, and RUMIANTCEV, conspired with one another and with others known and unknown to the Grand Jury to obtain unauthorized access to the computer networks of Filing Agent 1 and Filing Agent 2 using stolen employee credentials, and to view or download the financial disclosures of hundreds of publicly traded companies, including quarterly and annual reports that had not yet been filed with the SEC or disclosed to the public. Armed with these reports, which contained material non-public information, the defendants further conspired to enrich themselves by trading in the securities of those companies. Through this scheme, the defendants earned tens of millions of dollars in illegal profits.

Objects and Purposes of the Conspiracy

13. The objects of the conspiracy were to obtain unauthorized access to computers with intent to defraud, and to commit wire fraud and securities fraud. The principal purposes of the conspiracy were (1) to obtain material non-public information about the financial performance of publicly traded companies, (2) to enrich the conspirators by trading securities on the basis of that

HIGHLY SENSITIVE DOCUMENT

information, and (3) to conceal the conspirators' actions from their victims, securities regulators and law enforcement.

Manner and Means of the Conspiracy and the Scheme to Defraud

14. Among the manner and means by which the defendants, KLYUSHIN, ERMAKOV, and RUMLIANTCEV, together with others known and unknown to the Grand Jury, carried out the conspiracy and the scheme to defraud were the following:

- a. obtaining unauthorized access to the computer networks of Filing Agent 1 and Filing Agent 2;
- b. deploying malicious infrastructure capable of harvesting employees' usernames and passwords;
- c. using stolen usernames and passwords to misrepresent themselves as employees of Filing Agent 1 and Filing Agent 2 in order to obtain access to the filing agents' computer networks;
- d. leasing proxy (or intermediary) computer networks outside of Russia that obscured the origin of their attacks;
- e. subscribing to email addresses and payment systems used in furtherance of the attacks in others' names;
- f. once inside the filing agent networks, viewing or downloading material, non-public financial information—including quarterly and annual earnings reports that had not yet been filed with the SEC or disclosed to the general

HIGHLY SENSITIVE DOCUMENT

- public—of hundreds of companies that are publicly traded on U.S. national securities exchanges, including the NASDAQ and the NYSE;
- g. trading in the securities of those companies while in possession of material non-public information concerning their financial performance, including by purchasing securities of companies that were about to disclose positive financial results, and selling short securities of companies that were about to disclose negative financial results;
 - h. distributing their trading across accounts they opened at banks and brokerages in several countries, including Cyprus, Denmark, Portugal, Russia and the United States; and
 - i. misleading brokerage firms about, among other things, the nature of their trading activities.

Overt Acts in Furtherance of the Conspiracy

15. Beginning at least as early as January 2018 and continuing through at least September 2020, the defendants, KLYUSHIN, ERMAKOV, RUMIANTCEV, together with others known and unknown to the Grand Jury, committed and caused to be committed the following overt acts, among others, in furtherance of the conspiracy:

16. On or about February 5, 2018, ERMAKOV or another conspirator used the username and password of an employee of Filing Agent 2 (the “FA 2 Employee Credentials”) to obtain unauthorized access to the company’s computer network and to access earnings-related information of Snap, Inc., a company that is publicly traded on the NYSE. The information

HIGHLY SENSITIVE DOCUMENT

included a press release announcing Snap's fourth quarter and full year 2017 financial results that had not yet been filed with the SEC or publicly disclosed.

17. On or about February 6, 2018, Co-Conspirator 2 ("CC-2"), an individual whose identity is known to the Grand Jury, viewed the SNAP press release on his computer screen at approximately 8:13 a.m. (ET), more than eight hours before the results were filed with the SEC or publicly disclosed.

18. On or about May 9, 2018, starting at approximately 3:46 a.m. (ET), ERMAKOV used the FA 2 Employee Credentials to obtain unauthorized access to the computer network of Filing Agent 2 and to access earnings-related files of at least four companies: Cytomx Therapeutics, Inc., Horizon Therapeutics plc, Puma Biotechnology, Inc., and Synaptics Inc. All four companies are publicly traded on the NASDAQ, and reported their quarterly earnings later that day.

19. On or about October 22, 2018, ERMAKOV or another conspirator used the FA 2 Employee Credentials to obtain unauthorized access to the computer network of Filing Agent 2 through an IP address hosted at a data center located in Boston, Massachusetts and to view the quarterly financial results of Capstead Mortgage Corp. ("Capstead"), the securities of which are publicly traded on the NYSE. The Capstead results had not yet been filed with the SEC or publicly disclosed.

20. On or about October 23, 2018, KLYUSHIN or another conspirator shorted securities of Capstead in a brokerage account in KLYUSHIN's name at a Russia-based brokerage firm with operations in Cyprus (the "Russia-based brokerage firm").

HIGHLY SENSITIVE DOCUMENT

21. On or about October 24, 2018—shortly before Capstead publicly disclosed financial results that fell short of market expectations—Co-Conspirator 1 (“CC-1”), an individual whose identity is known to the Grand Jury, shorted shares of Capstead in an account in CC-1’s name at a U.S.-based brokerage firm.

22. On or about October 24, 2018, ERMAKOV or another conspirator used the FA 2 Employee Credentials to obtain unauthorized access to the computer network of Filing Agent 2 via another Boston IP address (collectively, the “Boston IP Addresses”), and to view the quarterly financial results of Tesla, Inc. (“Tesla”), the securities of which are publicly traded on the NASDAQ.

23. On or about that same day, before Tesla publicly disclosed positive quarterly earnings results:

- a. KLYUSHIN or another conspirator purchased Tesla securities in KLYUSHIN’s brokerage account at the Russia-based brokerage firm;
- b. KLYUSHIN sent the following message to Individual 1 and Individual 2: “Pay attention to shares of Tesla now and tomorrow after 16:30 and on how much they go up.”; and
- c. CC-1 purchased shares of Tesla in the U.S. brokerage account in his name.

24. On or about May 25, 2019, KLYUSHIN wrote to ERMAKOV, in substance, that they had accrued profits of close to \$1 million in the account of Individual 2 over the prior seven-month period, nearly tripling his investment, and profits of close to \$700,000 in the account of

HIGHLY SENSITIVE DOCUMENT

Individual 1, nearly doubling his investment of \$1 million. KLYUSHIN stated: “They don’t even ask why so anymore [smile].”

25. On or about June 13, 2019, KLYUSHIN sent a message to ERMAKOV in which he referred to RUMIANTCEV by the nickname “Kolya” and noted: “Kolya’s assets have grown [three smiles].” ERMAKOV responded: “Yes [smile].”

26. On or about the same day, KLYUSHIN told Individual 3: “I had a good day today[.] We made 1.2 million dollars on [trades] in the stock exchange and passed on 70 in suitcase [smile.] I did my deed[.]”

27. On or about July 28, 2019 and July 29, 2019, ERMAKOV or another conspirator used the FA 2 Employee Credentials to obtain unauthorized access to the computer network of Filing Agent 2 and to view earnings-related files of SS&C Technologies, Inc. (“SSNC”), the securities of which are publicly traded on the NASDAQ.

28. On or about July 29, 2019, shortly before SSNC reported second quarter financial results and lowered its profit forecast:

- a. CC-1 shorted SSNC shares in his U.S. brokerage account;
- b. Either CC-1 or CC-2 shorted contracts for difference (“CFDs”) in SSNC in an account that CC-1 and CC-2 had opened jointly in CC-1’s name at a Denmark-based bank specializing in online trading. CFDs are a type of security that allow traders to participate in the price movement of U.S. stocks without actually owning the underlying shares;

HIGHLY SENSITIVE DOCUMENT

- c. CC-2 shorted SSNC securities in a brokerage account in his own name at a second Russia-based financial services company with operations in Cyprus;
- d. KLYUSHIN or another conspirator sold short 11,800 SSNC CFDs in an account in KLYUSHIN's name at the Denmark-based bank; and
- e. KLYUSHIN, ERMAKOV or RUMIANTCEV shorted shares of SSNC in accounts in the names of Individual 1 and Individual 2 at the Russia-based brokerage firm.

29. On or about July 30, 2019, after SSNC publicly reported second quarter financial results and lowered its profit forecast, KLYUSHIN or another co-conspirator covered the entire SSNC short position in KLYUSHIN's account for a profit of approximately \$114,000.

30. On or about August 28, 2019, KLYUSHIN executed a power of attorney giving RUMIANTCEV authority to place trades in KLYUSHIN's account at the Denmark-based bank.

31. On or about August 29 and 30, 2019, KLYUSHIN shared photographs with ERMAKOV showing a safe that contained growing stacks of U.S. one hundred dollar bills.

32. On or about November 1, 2019, and again between November 4 and November 6, 2019, ERMAKOV or another conspirator used the FA 2 Employee Credentials to obtain unauthorized access to the computer network of Filing Agent 2 and to view earnings-related files of Roku Inc., the securities of which are publicly traded on the NASDAQ.

33. On or about November 6, 2019, hours before Roku reported third quarter financial results and reduced its profit forecasts, KLYUSHIN or another conspirator sold short 42,500 Roku CFDs in KLYUSHIN's account at the Denmark-based bank.

HIGHLY SENSITIVE DOCUMENT

34. On or about November 7, 2019, after Roku publicly reported its third quarter financial results, KLYUSHIN or another conspirator covered KLYUSHIN's Roku CFD short position for a profit of approximately \$1 million.

35. On or about November 19, 2019, RUMLIANTCEV received a text message from an employee of the Russia-based brokerage firm advising him, in substance, that his trading account and a few other clients' accounts were being blocked for suspicious transactions.

36. On or about January 21, 2020, ERMAKOV or another conspirator used the username and password of an employee of Filing Agent 1 (the "FA 1 Employee Credentials") to obtain unauthorized access to the company's computer network and to view earnings-related files of Avnet, Inc., the securities of which are publicly traded on the NASDAQ.

37. On or about January 23, 2020—hours before Avnet reported second quarter financial results that fell short of market expectations—ERMAKOV used a mobile trading application to access KLYUSHIN's account at the Denmark-based bank to short Avnet via CFDs.

38. On or about the same day, still before Avnet reported its second quarter financial results, CC-1 shorted Avnet shares in his U.S.-based brokerage account.

39. In a conference call on or about April 24, 2020, KLYUSHIN and RUMLIANTCEV falsely told an employee of the Denmark-based bank, in substance, that M-13 traded on the basis of its analysis of publicly available information, including historical data and social media postings, and not on the basis of material non-public information.

HIGHLY SENSITIVE DOCUMENT

40. On or about September 17, 2020, RUMIANTCEV told KLYUSHIN that M-13 would earn approximately \$522,000 based on its profitable trading on behalf of Individual 2 during the third quarter of 2020, representing 60 percent of the profits earned on those trades.

41. On or about the following day, RUMIANTCEV told KLYUSHIN that M-13 would earn approximately \$443,700 based on its profitable trading on behalf of Individual 3 during the third quarter of 2020, representing 60 percent of the profits earned on those trades.

HIGHLY SENSITIVE DOCUMENT

COUNT ONE

Conspiracy to Obtain Unauthorized Access to Computers,
and to Commit Wire Fraud and Securities Fraud
(18 U.S.C. § 371)

The Grand Jury charges:

42. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 41 of this Indictment.

43. From in or about at least January 2018 through in or about at least September 2020, in the District of Massachusetts and elsewhere, the defendants,

VLADISLAV KLYUSHIN,
a/k/a "Vladislav Kliushin,"
IVAN ERMAKOV,
a/k/a "Ivan Yermakov," and
NIKOLAI RUMIANTCEV,
a/k/a "Nikolay Rummyantsev,"

conspired with one another, and with others known and unknown to the Grand Jury, to commit offenses against the United States, to wit:

- a. computer intrusion, in violation of Title 18, United States Code, Section 1030(a)(4), that is, to knowingly access a protected computer without authorization, with intent to defraud, and by means of such conduct to further the intended fraud and obtain a thing of value;
- b. wire fraud, in violation of Title 18, United States Code, Section 1343, to wit: having devised and intending 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 transmit and cause to

HIGHLY SENSITIVE DOCUMENT

be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures and sounds for the purpose of executing the scheme to defraud; and

- c. securities fraud, in violation of Title 15, United States Code, Sections 78j(b) and 78ff(a), and Title 17, Code of Federal Regulations, Section 240.10b-5, to wit: knowingly and willfully, by the use of means and instrumentalities of interstate commerce, the mails, and the facilities of a national securities exchange, directly and indirectly to use and employ manipulative and deceptive devices and contrivances in connection with the purchase and sale of securities, in contravention of Rule 10b-5 of the Rules and Regulations promulgated by the United States Securities and Exchange Commission, by: (a) employing devices, schemes and artifices to defraud; (b) making untrue statements of material facts and omitting to state material facts necessary in order to make the statements made, in light of circumstances under which they were made, not misleading; and (c) engaging in acts, practices and courses of business which would and did operate as a fraud and deceit in connection with the purchase and sale of securities.

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

HIGHLY SENSITIVE DOCUMENT

COUNT TWO

Wire Fraud; Aiding and Abetting
(18 U.S.C. §§ 1343 and 2)

The Grand Jury further charges:

44. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 41 of this Indictment.

45. On or about October 24, 2018, in the District of Massachusetts and elsewhere, the defendants,

VLADISLAV KLYUSHIN,
a/k/a "Vladislav Kliushin,"
IVAN ERMAKOV,
a/k/a "Ivan Yermakov," and
NIKOLAI RUMIANTCEV,
a/k/a "Nikolay Rumyantsev,"

together with others known and unknown to the Grand Jury, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property, to wit, the confidential financial information of Tesla, Capstead and other publicly traded clients of Filing Agent 2, by means of materially false and fraudulent pretenses, representations, and promises, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing the scheme to defraud, specifically: the FA 2 Employee Credentials, which were transmitted, via the Boston IP Addresses, to one or more computer servers outside of Massachusetts in order to obtain unauthorized access to the computer network of Filing Agent 2.

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

HIGHLY SENSITIVE DOCUMENT

COUNT THREE

Unauthorized Access to Computers; Aiding and Abetting
(18 U.S.C. §§ 1030(a)(4) and 2))

The Grand Jury further charges:

46. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 41 of this Indictment.

47. On or about October 24, 2018, in the District of Massachusetts and elsewhere, the defendants,

VLADISLAV KLYUSHIN,
a/k/a "Vladislav Kliushin,"
IVAN ERMAKOV,
a/k/a "Ivan Yermakov," and
NIKOLAI RUMIANTCEV,
a/k/a "Nikolay Rumyantsev,"

together with others known and unknown to the Grand Jury, did knowingly access a protected computer without authorization, with intent to defraud, and by means of such conduct did further the intended fraud and obtain a thing of value, to wit: the confidential financial information of Tesla, Capstead, and other publicly traded clients of Filing Agent 2.

All in violation of Title 18, United States Code, Sections 1030(a)(4) and 2.

HIGHLY SENSITIVE DOCUMENT

COUNT FOUR

Securities Fraud; Aiding and Abetting
(15 U.S.C. §§ 78j(b) and 78ff(a); 17 C.F.R. § 240.10b 5; 18 U.S.C. § 2)

The Grand Jury further charges:

48. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 41 of this Indictment.

49. On various dates between on or about February 5, 2018 and on or about January 23, 2020, in the District of Massachusetts and elsewhere, the defendants,

VLADISLAV KLYUSHIN,
a/k/a "Vladislav Kliushin,"
IVAN ERMAKOV,
a/k/a "Ivan Yermakov," and
NIKOLAI RUMIANTCEV,
a/k/a "Nikolay Rumyantsev,"

together with others known and unknown to the Grand Jury, did knowingly and willfully, by the use of means and instrumentalities of interstate commerce, the mails, and the facilities of national securities exchanges, directly and indirectly use and employ manipulative and deceptive devices and contrivances in connection with the purchase and sale of securities in contravention of Rule 10b-5 (17 C.F.R. § 240.10b-5) of the Rules and Regulations promulgated by the United States Securities and Exchange Commission, and did (a) employ a device, scheme and artifice to defraud, (b) make untrue statements of material facts and omit to state material facts necessary in order to make the statements made, in light of circumstances under which they were made, not misleading, and (c) engage in acts, practices and a course of business which would and did operate as a fraud

HIGHLY SENSITIVE DOCUMENT

and deceit, in connection with the purchase and sale of securities, specifically, the securities of publicly traded companies that were clients of Filing Agent 2.

All in violation of Title 15, United States Code, Sections 78j(b) & 78ff(a); Title 17, Code of Federal Regulations, Section 240.10b-5; and Title 18, United States Code, Section 2.

HIGHLY SENSITIVE DOCUMENT

FORFEITURE ALLEGATION
(18 U.S.C. § 981(a)(1)(C) & 28 U.S.C. § 2461(c))

50. Upon conviction of one or more of the offenses charged in Counts One, Two and Four of this Indictment, the defendants,

VLADISLAV KLYUSHIN,
a/k/a "Vladislav Kliushin,"
IVAN ERMAKOV,
a/k/a "Ivan Yermakov," and
NIKOLAI RUMIANTCEV,
a/k/a "Nikolay Rumyantsev,"

shall forfeit to the United States pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c), any property, real or personal, which constitutes or is derived from proceeds traceable to such offenses.

51. If any of the property described in paragraph 50 above, as being forfeitable pursuant to Title 18, United States Code, Section 981(a)(1)(C), and Title 28, United States Code, Section 2461(c), as a result of any act or omission by the defendants,

- 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,

HIGHLY SENSITIVE DOCUMENT

it is the intention of the United States, pursuant to Title 28, United States Code, Section 2461(c), incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the property described in paragraph 50 above.

All pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461(c).

HIGHLY SENSITIVE DOCUMENT

COMPUTER INTRUSION FORFEITURE ALLEGATION
(18 U.S.C. §§ 982(a)(2)(B) & 1030(i))

52. Upon conviction of one or more of the offenses in violation of Title 18, United States Code, Sections 371 and 1030(a), set forth in Counts One and Three, the defendants,

VLADISLAV KLYUSHIN,
a/k/a "Vladislav Kliushin,"
IVAN ERMAKOV,
a/k/a "Ivan Yermakov," and
NIKOLAI RUMLIANTCEV,
a/k/a "Nikolay Rumyantsev,"

shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(B) and 1030(i), any property constituting or derived from any proceeds obtained, directly or indirectly, as a result of such offenses; and, pursuant to Title 18, United States Code Section 1030(i), any personal property used, or intended to be used, to commit, or to facilitate the commission of, such offenses and any property, real or personal, constituting or derived from any proceeds obtained, directly or indirectly, as a result of such offenses.

53. If any of the property described in Paragraph 52, above, as being forfeitable pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), as a result of any act or omission of the defendants --

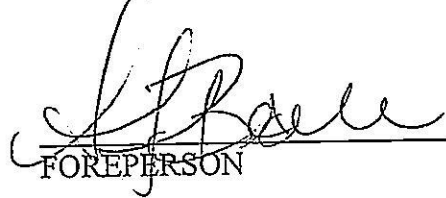
- a. cannot be located upon the exercise of due diligence;
- b. has been transferred or sold to, or deposited with, a third party;
- c. has been placed beyond the jurisdiction of the Court;
- d. has been substantially diminished in value; or
- e. has been commingled with other property which cannot be divided without difficulty;


HIGHLY SENSITIVE DOCUMENT

it is the intention of the United States, pursuant to Title 18, United States Code, Sections 982(b)(2) and 1030(i)(2), each incorporating Title 21, United States Code, Section 853(p), to seek forfeiture of any other property of the defendants up to the value of the property described in Paragraph 52 above.

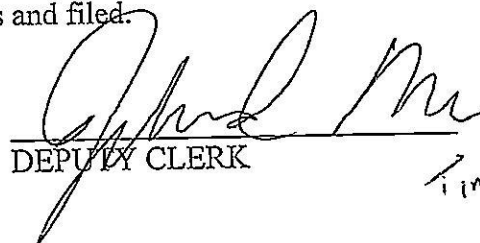
All pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i).

A TRUE BILL


FOREPERSON


STEPHEN E. FRANK
SETH B. KOSTO
ASSISTANT UNITED STATES ATTORNEYS
DISTRICT OF MASSACHUSETTS

District of Massachusetts: April 6, 2020
Returned into the District Court by the Grand Jurors and filed.


DEPUTY CLERK
Time: 1:53pm

HIGHLY SENSITIVE DOCUMENTS

JS 45 (5/97) - (Revised U.S.D.C. MA 3/25/2011)

Criminal Case Cover Sheet

U.S. District Court - District of Massachusetts

Place of Offense: _____ Category No. II Investigating Agency FBI

City BOSTON Related Case Information:

County Suffolk Superseding Ind./ Inf. _____ Case No. _____
Same Defendant _____ New Defendant _____
Magistrate Judge Case Number 21-MJ-2090-MBB
Search Warrant Case Number 20-MJ-2221-MBB
R 20/R 40 from District of _____

Defendant Information:

Defendant Name VLADISLAV KLYUSHIN Juvenile: Yes No

Is this person an attorney and/or a member of any state/federal bar: Yes No

Alias Name VLADISLAV KLIUSHIN

Address (City & State) RUSSIAN FEDERATION

Birth date (Yr only): 1980 SSN (last4#): _____ Sex M Race: WHITE Nationality: RUSSIAN

Defense Counsel if known: _____ Address _____

Bar Number _____

U.S. Attorney Information:

AUSA Seth B. Kosto and Stephen E. Frank Bar Number if applicable _____

Interpreter: Yes No List language and/or dialect: Russian

Victims: Yes No If yes, are there multiple crime victims under 18 USC§3771(d)(2) Yes No

Matter to be SEALED: Yes No

Warrant Requested Regular Process In Custody

Location Status:

Arrest Date _____

Already in Federal Custody as of _____ in _____

Already in State Custody at _____ Serving Sentence Awaiting Trial

On Pretrial Release: Ordered by: _____ on _____

Charging Document: Complaint Information Indictment

Total # of Counts: Petty _____ Misdemeanor _____ Felony 4

Continue on Page 2 for Entry of U.S.C. Citations

I hereby certify that the case numbers of any prior proceedings before a Magistrate Judge are accurately set forth above.

Date: 04/06/2021 Signature of AUSA: _____

HSD
DOCKETED

8

District Court Case Number (To be filled in by deputy clerk): _____

Name of Defendant _____

U.S.C. Citations

	<u>Index Key/Code</u>	<u>Description of Offense Charged</u>	<u>Count Numbers</u>
Set 1	18 U.S.C. § 371	Conspiracy to Obtain Unauthorized Access to Computers, and to Commit Wire Fraud and Securites Fraud.	Count One
Set 2	18 U.S.C. §§ 1343 and 2	Wire Fraud; Aiding and Abetting.	Count Two
Set 3	18 U.S.C. §§ 1030(a)(4) and 2	Unauthorized Access to Computers; Aiding and Abetting.	Count Three
Set 4	15 U.S.C. §§ 78j(b) and 78ff(a); 17 C.F.R. § 240.10b-5; 18 U.S.C. § 2	Securities Fraud; Aiding and Abetting.	Count Four
Set 5	18 U.S.C. §§ 981(a)(1)(C) and 28 U.S.C. § 2461(c)	Forfeiture Allegation	
Set 6	18 U.S.C. §§ 982(a)(2)(B) and 1030(i)	Computer Intrusion Forfeiture Allegation	
Set 7			
Set 8			
Set 9			
Set 10			
Set 11			
Set 12			
Set 13			
Set 14			
Set 15			
ADDITIONAL INFORMATION: _____			

Criminal Case Cover Sheet

Place of Offense: _____ Category No. II Investigating Agency FBI

City BOSTON Related Case Information:

County Suffolk Superseding Ind./ Inf. _____ Case No. _____
Same Defendant _____ New Defendant _____
Magistrate Judge Case Number 21-MJ-2090-MBB
Search Warrant Case Number 20-MJ-2221-MBB
R 20/R 40 from District of _____

Defendant Information:

Defendant Name NIKOLAI RUMIANTCEV Juvenile: Yes No

Is this person an attorney and/or a member of any state/federal bar: Yes No

Alias Name NIKOLAY RUMYANTSEV

Address (City & State) RUSSIAN FEDERATION

Birth date (Yr only): 1988 SSN (last4#): _____ Sex M Race: WHITE Nationality: RUSSIAN

Defense Counsel if known: _____ Address _____

Bar Number _____

U.S. Attorney Information:

AUSA Seth B. Kosto and Stephen E. Frank Bar Number if applicable _____

Interpreter: Yes No List language and/or dialect: Russian

Victims: Yes No If yes, are there multiple crime victims under 18 USC§3771(d)(2) Yes No

Matter to be SEALED: Yes No

Warrant Requested Regular Process In Custody

DOCKETED
HSD

Location Status:

Arrest Date _____

Already in Federal Custody as of _____ in _____

Already in State Custody at _____ Serving Sentence Awaiting Trial

On Pretrial Release: Ordered by: _____ on _____

Charging Document: Complaint Information Indictment

Total # of Counts: Petty _____ Misdemeanor _____ Felony 4

Continue on Page 2 for Entry of U.S.C. Citations

I hereby certify that the case numbers of any prior proceedings before a Magistrate Judge are accurately set forth above.

Date: 04/06/2021 Signature of AUSA: _____

8

District Court Case Number (To be filled in by deputy clerk): _____

Name of Defendant _____

U.S.C. Citations

	<u>Index Key/Code</u>	<u>Description of Offense Charged</u>	<u>Count Numbers</u>
Set 1	18 U.S.C. § 371	Conspiracy to Obtain Unauthorized Access to Computers, and to Commit Wire Fraud and Securites Fraud.	Count One
Set 2	18 U.S.C. §§ 1343 and 2	Wire Fraud; Aiding and Abetting.	Count Two
Set 3	18 U.S.C. §§ 1030(a)(4) and 2	Unauthorized Access to Computers; Aiding and Abetting.	Count Three
Set 4	15 U.S.C. §§ 78j(b) and 78ff(a); 17 C.F.R. § 240.10b-5; 18 U.S.C. § 2	Securities Fraud; Aiding and Abetting.	Count Four
Set 5	18 U.S.C. §§ 981(a)(1)(C) and 28 U.S.C. § 2461(c)	Forfeiture Allegation	
Set 6	18 U.S.C. §§ 982(a)(2)(B) and 1030(i)	Computer Intrusion Forfeiture Allegation	
Set 7	_____	_____	_____
Set 8	_____	_____	_____
Set 9	_____	_____	_____
Set 10	_____	_____	_____
Set 11	_____	_____	_____
Set 12	_____	_____	_____
Set 13	_____	_____	_____
Set 14	_____	_____	_____
Set 15	_____	_____	_____

ADDITIONAL INFORMATION: _____

Criminal Case Cover Sheet

U.S. District Court - District of Massachusetts

Place of Offense: _____ Category No. II Investigating Agency FBI

City BOSTON Related Case Information:

County Suffolk Superseding Ind./ Inf. _____ Case No. _____
Same Defendant _____ New Defendant _____
Magistrate Judge Case Number 21-MJ-2090-MBB
Search Warrant Case Number 20-MJ-2221-MBB
R 20/R 40 from District of _____

Defendant Information:

Defendant Name IVAN ERMAKOV Juvenile: Yes No
Is this person an attorney and/or a member of any state/federal bar: Yes No

Alias Name IVAN YERMAKOV
Address (City & State) RUSSIAN FEDERATION

only): 1986 SSN (last4#): _____ Sex M Defense Counsel if _____ Race: WHITE Nationality: RUSSIAN

known: _____ Address _____

Bar Number _____

U.S. Attorney Information:

AUSA Seth B. Kosto and Stephen E. Frank Bar Number if applicable _____

Interpreter: Yes No List language and/or dialect: Russian

Victims: Yes No If yes, are there multiple crime victims under 18 USC§3771(d)(2) Yes No

Matter to be SEALED: Yes No

Warrant Requested Regular Process In Custody

Location Status:

Arrest Date _____

Already in Federal Custody as of _____ in _____

Already in State Custody at _____ Serving Sentence Awaiting Trial

On Pretrial Release: Ordered by: _____ on _____

Charging Document: Complaint Information Indictment

Total # of Counts: Petty _____ Misdemeanor _____ Felony 4

Continue on Page 2 for Entry of U.S.C. Citations

I hereby certify that the case numbers of any prior proceedings before a Magistrate Judge are accurately set forth above.

Date: 04/06/2021 Signature of AUSA: _____

HSD DOCKETED

District Court Case Number (To be filled in by deputy clerk): _____

Name of Defendant _____

U.S.C. Citations

	<u>Index Key/Code</u>	<u>Description of Offense Charged</u>	<u>Count Numbers</u>
Set 1	<u>18 U.S.C. § 371</u>	<u>Conspiracy to Obtain Unauthorized Access to Computers, and to Commit Wire Fraud and Securites Fraud.</u>	<u>Count One</u>
Set 2	<u>18 U.S.C. §§ 1343 and 2</u>	<u>Wire Fraud; Aiding and Abetting.</u>	<u>Count Two</u>
Set 3	<u>18 U.S.C. §§ 1030(a)(4) and 2</u>	<u>Unauthorized Access to Computers; Aiding and Abetting.</u>	<u>Count Three</u>
Set 4	<u>15 U.S.C. §§ 78j(b) and 78ff(a); 17 C.F.R. § 240.10b-5; 18 U.S.C. § 2</u>	<u>Securities Fraud; Aiding and Abetting.</u>	<u>Count Four</u>
Set 5	<u>18 U.S.C. §§ 981(a)(1)(C) and 28 U.S.C. § 2461(c)</u>	<u>Forfeiture Allegation</u>	
Set 6	<u>18 U.S.C. §§ 982(a)(2)(B) and 1030(i)</u>	<u>Computer Intrusion Forfeiture Allegation</u>	
Set 7	_____	_____	_____
Set 8	_____	_____	_____
Set 9	_____	_____	_____
Set 10	_____	_____	_____
Set 11	_____	_____	_____
Set 12	_____	_____	_____
Set 13	_____	_____	_____
Set 14	_____	_____	_____
Set 15	_____	_____	_____

ADDITIONAL INFORMATION: _____

UNITED STATES DISTRICT COURT
DISTRICT OF
MASSACHUSETTS

PLACEHOLDER FOR
HSD Case

USA

Plaintiff(s)

v.

Case Number: 21-cr-10104

John Doe 1, 2, and 5

Defendant(s)

**PLEASE USE THIS PLACEHOLDER TO FILE
SEALED DOCUMENTS WITH HIGHLY SENSITIVE INFORMATION (HSI)
IN BOTH CIVIL AND CRIMINAL CASES**

INSTRUCTIONS:

- 1) FILE - File this placeholder in ECF in place of a sealed document with highly sensitive information (HSI) using the normal ECF event you would use to file a sealed document.
- 2) PRINT, ATTACH & SEAL- Print the filed placeholder from ECF as well as a copy of the NEF (Notice of Electronic Filing). Attach both documents to the sealed document with HSI. Place inside of an envelope marked "SEALED HIGHLY SENSITIVE DOCUMENT."
- 3) DELIVER – Contemporaneously with the filing of the Placeholder Form in ECF, deliver or place in the mail the envelopes to the Clerk's Office.
- 4) COURTESY COPIES - Provide a courtesy copy to the presiding judge.