HIGHLY SENSITIVE DOCUMENT

HSD

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA v. MIKHAIL VLADIMIROVICH IRZAK, a/k/a "Mikka Irzak," and IGOR SERGEEVICH SLADKOV, Defendants	Criminal No. 21-10146-NMG Violations: Count One: Conspiracy to Gain Unauthorized Access to Computers, and to Commit Wire Fraud and Securities Fraud (18 U.S.C. § 371) Count Two: 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 MIKHAIL VLADIMIROVICH IRZAK, also known as "Mikka Irzak," was a Russian citizen who resided in St. Petersburg, Russia.

2. Defendant IGOR SERGEEVICH SLADKOV was a Russian citizen who resided in St. Petersburg, Russia.

3. IRZAK had a brokerage account in his own name at Financial Services Company A, a retail brokerage firm with operations in the United States. IRZAK and SLADKOV also

Denmark-based investment bank that specializes in online trading. SLADKOV held brokerage accounts in his own name at Financial Services Company C, which operates in Cyprus and Russia.

4. Co-Conspirator 1 (CC-1) was a Russian citizen who resided in Moscow, Russia. CC-1 was employed as a deputy general director of M-13, a company based in Moscow that 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 gain 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."

6. 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.

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

8. 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.

9. 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.

10. 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.

HIGHLY SENSITIVE DOCUMENT

Overview of the Conspiracy and the Scheme to Defraud

11. Beginning at least as early as February 2018 and continuing through at least September 2020, the defendants, IRZAK and SLADKOV, conspired with one another, with CC-1, 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 log-in credentials, and to view and 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

12. The objects of the conspiracy were to gain 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 information, and (3) to conceal the conspirators' actions from their victims, securities regulators and law enforcement.

HIGHLY SENSITIVE DOCUMENT

Manner and Means of the Conspiracy and the Scheme to Defraud

13. Among the manner and means by which the defendants, IRZAK and SLADKOV, CC-1, and 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 gain 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 agents' networks, viewing and 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 public—of hundreds of companies that are publicly traded on U.S. national securities exchanges, including the NASDAQ and the NYSE; and

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.

Overt Acts in Furtherance of the Conspiracy

14. Beginning at least as early as February 2018 and continuing through at least September 2020, the defendants, IRZAK and SLADKOV, CC-1, and 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:

15. On or about February 5, 2018, CC-1 or another conspirator used the username and password of an employee of Filing Agent 2 (the FA 2 Employee Credentials) to gain 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 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.

16. On or about February 6, 2018, SLADKOV viewed the Snap earnings 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.

17. On or about the morning of July 24, 2018, CC-1 or another conspirator used the FA 2 Employee Credentials to gain unauthorized access to the computer network of Filing Agent 2

and to view earnings-related files of seven publicly traded companies: Grubhub, Inc., Patterson-UTI Energy, Inc., Ultra Clean Holdings, Inc., CNH Industrial N.V., Getty Realty Corp., Essendant, Inc., and The Nielsen Company, all of which reported their quarterly earnings over the following two days.

18. Later that same day—one day before Grubhub reported second quarter financial results that exceeded market expectations—IRZAK or SLADKOV purchased 1,700 Grubhub contracts for difference (CFDs) in the account in IRZAK's name at Financial Services Company B. 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.

19. Likewise, on or about July 25, 2018—one day before The Nielsen Company reported second quarter financial results that missed market estimates—IRZAK or SLADKOV sold short 8,500 CFDs in The Nielsen Company in the account at Financial Services Company B.

20. SLADKOV also placed trades in each of the seven companies in one of his accounts at Financial Services Company C before any of the companies publicly disclosed their second quarter financial results.

21. On or about October 22, 2018, CC-1 or another conspirator used the FA 2 Employee Credentials to gain 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.

22. On or about October 24, 2018—shortly before Capstead publicly disclosed financial results that fell short of market expectations—IRZAK shorted 5,000 shares of Capstead in his account at Financial Services Company A.

23. On or about October 24, 2018, CC-1 or another conspirator used the FA 2 Employee Credentials to gain unauthorized access to the computer network of Filing Agent 2 via another Boston IP address and to view the quarterly financial results of Tesla, Inc. (Tesla), the securities of which are publicly traded on the NASDAQ.

24. On or about that same day, before Tesla publicly disclosed positive quarterly earnings results, IRZAK purchased 200 shares of Tesla in his account at Financial Services Company A, and IRZAK or SLADKOV purchased Tesla CFDs in the account at Financial Services Company B.

25. On or about February 25, 2019 and February 26, 2019, CC-1 or another conspirator used the FA 2 Employee Credentials to gain unauthorized access to the computer network of Filing Agent 2 and to view the quarterly financial results of Tandem Diabetes Care (Tandem), which had not yet been filed with the SEC or publicly disclosed.

26. On or about those same days, before Tandem announced positive fourth quarter and full-year 2018 financial results after the close of the market on February 26, 2019:

a. SLADKOV purchased 33,000 shares of Tandem in one of his accounts at Financial Services Company C;

b. IRZAK purchased 2,000 shares of Tandem in his account at Financial Services Company A; and

c. IRZAK or SLADKOV purchased 2,000 Tandem CFDs in the account at Financial Services Company B,

27. On or about May 20, 2019, between 8:28 a.m. and 8:30 a.m. (ET), CC-1 or another conspirator used the FA 2 Employee Credentials to gain unauthorized access to the computer network of Filing Agent 2 and to view the quarterly financial results of Kohl's Corp.

28. Beginning at 9:50 a.m. (ET) that same day, SLADKOV opened a short position in Kohl's in one of his accounts at Financial Services Company C.

29. Beginning at approximately 10:01 a.m. (ET) that same day, IRZAK opened a short position in Kohl's in his account at Financial Services Company A.

30. At or about the same time, IRZAK or SLADKOV also opened a short position in Kohl's in the account at Financial Services Company B.

31. On or about the following day, May 21, 2019, after Kohl's publicly announced financial results that fell below analyst expectations, prompting its share price to fall, IRZAK covered his short position at Financial Services Company A, earning an overnight profit of approximately $41,000.

32. Likewise, IRZAK or SLADKOV covered the short position at Financial Services Company B, earning an overnight profit of approximately $29,000.

33. SLADKOV also covered his short position at Financial Services Company C, earning an overnight profit of approximately $400,000.

34. That same day, SLADKOV and CC-1 shared screenshots showing Kohl's share prices.

35. On or about July 28, 2019 and July 29, 2019, CC-1 or another conspirator used the FA 2 Employee Credentials to gain 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.

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

a. IRZAK shorted 10,000 SSNC shares in his account at Financial Services Company A;

b. IRZAK or SLADKOV shorted 16,000 CFDs in SSNC in the account at Financial Services Company B; and

c. SLADKOV shorted 179,739 SSNC shares in one of his accounts at Financial Services Company C.

37. On or about May 27, 2020, CC-1 or another conspirator gained unauthorized access to the computer network of Filing Agent 2 and viewed earnings-related files of Box, Inc., the securities of which are publicly traded on the NYSE.

38. Later that same day, IRZAK purchased approximately 20,000 Box shares in his account at Financial Services Company A.

39. At approximately 3:47 p.m. (ET)—shortly before Box reported quarterly earnings and revenue that exceeded market estimates—SLADKOV shared a screenshot with a representative of Financial Services Company C showing trading activity in Box in one of his accounts.

HIGHLY SENSITIVE DOCUMENT

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

The Grand Jury charges:

40. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 39 of this Indictment.

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

MIKHAIL VLADIMIROVICH IRZAK,
a/k/a "Mikka Irzak,"
and
IGOR SERGEEVICH SLADKOV,

conspired with one another, with CC-1, 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, that is, 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 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, that is, 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
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:

42. The Grand Jury re-alleges and incorporates by reference paragraphs 1 through 39 of this Indictment and further charges that:

43. 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,

MIKHAIL VLADIMIROVICH IRZAK,
a/k/a "Mikka Irzak,"
and
IGOR SERGEEVICH SLADKOV,

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 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.

HIGHLY SENSITIVE DOCUMENT

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))

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

MIKHAIL VLADIMIROVICH IRZAK,
a/k/a "Mikka Irzak,"
and
IGOR SERGEEVICH SLADKOV,

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.

45. If any of the property described in paragraph 44 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,

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 44 above.

HIGHLY SENSITIVE DOCUMENT

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))

46. Upon conviction of the offense in violation of Title 18, United States Code, Sections 371 and 1030(a), set forth in Count One, the defendants,

MIKHAIL VLADIMIROVICH IRZAK,
a/k/a "Mikka Irzak,"
and
IGOR SERGEEVICH SLADKOV,

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.

47. If any of the property described in Paragraph 46, 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;

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 46 above.

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

A TRUE BILL

[redacted]

FOREPERSON

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

District of Massachusetts: May 6, 2021
Returned into the District Court by the Grand Jurors and filed.

DEPUTY CLERK 2:18 PM.