DOCKETED
HSD

AFFIDAVIT

I, BJ Kang, being sworn, state:

INTRODUCTION AND AGENT BACKGROUND

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 2005. During that time, I have participated in numerous investigations of fraud relating to the securities markets, including accounting fraud, market manipulation, insider trading, and Ponzi schemes. I have conducted or participated in arrests, the execution of search warrants, surveillance, debriefings of informants, and reviews of recorded conversations and securities trading records. I am currently assigned to the FBI Washington Field Office ("WFO") criminal computer intrusion squad, where I investigate crimes involving computer intrusions and other cyber related matters. Before my assignment to WFO, I was a Supervisory Special Agent at FBI cyber headquarters, where I provided support to financially motivated cyber intrusion investigations. I have also received training in cybercrime investigation techniques, computer evidence identification, and analyzing and tracing digital currency.

2. I am a "federal law enforcement officer" within the meaning of Fed. R. Crim. P. 41(a)(2)(C), that is, a government agent authorized to enforce criminal laws and duly authorized by the Attorney General to execute warrants issued under the authority of the United States.

3. I make this affidavit in support of an application for a complaint charging VLADISLAV DMITRIYEVICH KLYUSHIN, also known as VLADISLAV KLIUSHIN, IVAN SERGEYEVICH ERMAKOV, also known as IVAN YERMAKOV, IGOR SERGEEVICH SLADKOV, MIKHAIL VLADIMIROVICH IRZAK, also known as MIKKA IRZAK, and NIKOLAI MIKHAYLOVICH RUMIANTCEV, also known as NIKOLAY RUMYANTSEV, with conspiracy to commit computer intrusion, wire fraud and securities fraud, in violation of

Title 18, United States Code, Section 371, and contrary to Title 18, United States Code, Sections 1030(a)(4) and 1343, and Title 15, United States Code, Sections 78j(b) and 78ff(a), respectively, and for warrants to arrest KLYUSHIN, ERMAKOV, IRZAK, SLADKOV and RUMIANTCEV on these charges.

4. I have personally participated in the investigation, and the facts in this affidavit come from, among other things, my personal observations, my training and experience, publicly available information, information obtained from the Securities and Exchange Commission ("SEC") and the Financial Industry Regulatory Authority ("FINRA"),[1] and information obtained through legal process, Court orders, and Court-authorized search warrants. Unless otherwise noted, all times are set forth in Moscow, Russia time and are approximate, and translations set forth herein are draft translations. This affidavit is intended to show that there is probable cause for the requested complaint and arrest warrants and does not set forth all of my knowledge about this matter.

OVERVIEW

5. As set forth below, between at least in or about 2018 and 2020, KLYUSHIN, ERMAKOV, SLADKOV, IRZAK, RUMIANTCEV, and others known and unknown conspired to trade in the securities of publicly traded companies based on material non-public information ("MNPI") about the earnings of those companies, in advance of the public announcements of those financial results. The MNPI was acquired through unauthorized intrusions into the

[1] FINRA is a private, not-for-profit corporation that acts as a self-regulatory organization for the brokerage industry. FINRA seeks to provide investor protection and ensure market integrity through regulation of broker-dealers.

computer networks of two U.S.-based filing agents—vendors that publicly traded companies use to make quarterly and annual filings through the SEC's EDGAR system.[2]

6. Armed with this information before it was disclosed to the public, KLYUSHIN, ERMAKOV, SLADKOV, IRZAK, RUMIANTCEV, and others knew ahead of time, among other things, whether a company's financial performance would meet, exceed, or lag market expectations—and thus whether its share price would likely rise or fall following the public announcement of that performance—and they traded accordingly, in brokerage accounts held in their own names and in the names of others.

7. In this fashion, KLYUSHIN, ERMAKOV, SLADKOV, IRZAK, and RUMIANTCEV made tens of millions of dollars in illegal profits.

BACKGROUND

8. At all times relevant to this affidavit:

a. KLYUSHIN, ERMAKOV, SLADKOV, IRZAK, and RUMIANTCEV were citizens of Russia.[3]

---

[2] EDGAR, the Electronic Data Gathering, Analysis, and Retrieval system, is an online database system maintained by the SEC, and accessible to the public, where publicly traded companies and filing agents file regulatory documents such as annual reports and quarterly earnings reports.

[3] On or about July 13, 2018, ERMAKOV and several Russian military intelligence officers were indicted in the United States District Court for the District of Columbia on various charges—including conspiracy, false registration of a domain name, aggravated identity theft, conspiracy to commit money laundering, conspiracy to commit computer fraud, conspiracy to commit wire fraud, and wire fraud—in connection with their alleged roles in interfering with the 2016 United States elections by way of computer hacking. Additionally, on or about October 3, 2018, ERMAKOV and several other Russian citizens were indicted in the United States District Court for the Western District of Pennsylvania on charges—including conspiracy to commit computer fraud, conspiracy to commit wire fraud, wire fraud, aggravated identity theft, and conspiracy to commit money laundering—in connection with their alleged roles in hacking and

b. KLYUSHIN, ERMAKOV, and RUMIANTCEV were employed by M-13 LLC ("M-13" or "M13"), which purported to be a Moscow, Russia-based information technology ("IT") company. Based on open-source research and my review of records obtained during the course of this investigation, I am aware that M-13 purports to provide, among other things, "monitoring and analytics of media and social media messages" and penetration testing services. Penetration testing, also called pen testing, is an authorized, simulated cyberattack that is used to evaluate an organization's ability to protect its computer system, network, 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. According to M-13's website, the company's "IT solutions" are 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." Based on my review of records obtained during the course of this investigation, I am aware that KLYUSHIN was M-13's first deputy general director, and ERMAKOV and RUMIANTCEV were deputy general directors.

c. IRZAK held an account in his own name at Interactive Brokers, LLC ("IB"), a retail brokerage firm with operations in the United States (the "IRZAK IB Account"), with Saxo Bank, a Denmark-based investment bank that specializes in online trading (the "IRZAK Saxo Account"), and with Millennium bcp, a Portugal-based bank that provides brokerage services (the "IRZAK Millennium Account").

---

related disinformation operations targeting international anti-doping agencies, sporting federations, and anti-doping officials.

d. SLADKOV held brokerage accounts in his own name at BrokerCreditService Ltd. ("BCS"), a financial services company with operations in Cyprus and Russia (the "SLADKOV BCS Accounts").

e. KLYUSHIN held a brokerage account in his own name at Saxo Bank (the "KLYUSHIN Saxo Account"). As set forth below, ERMAKOV sometimes executed trades in the KLYUSHIN Saxo Account.

f. Filing Agent 1 ("FA 1") and Filing Agent 2 ("FA 2") operated in the United States and accepted for filing through EDGAR quarterly and annual financial results from publicly traded companies before those results were made public.

Network Intrusions at FA 1

9. In or about January 2020, FA 1 reported to the FBI that its computer network had been compromised. FA 1 records suggest that the compromise began as early as November 2018.

10. According to FA 1, intruders gained access to the login credentials (*i.e.*, usernames and passwords) of one or more of its employees and used them to access the company's network without authorization and to view and/or download earnings-related files, including drafts of SEC filings and press releases, for several publicly traded companies.

11. For example, on or about January 21, 2020, between 8:58 a.m. and 9:34 a.m. (ET), an FA 1 employee's compromised login credentials were used to gain unauthorized access to drafts of earnings press releases of several publicly traded companies—including IBM Corp., Steel Dynamics, Inc., and Avnet, Inc.—before those companies announced their 2019 financial results after the market closed that day, and on January 22 and January 23, 2020, respectively.

Network Intrusions at FA 2

12. In or about January 2020, FA 2 likewise reported to the FBI that its computer network had been compromised using an FA 2 employee's compromised login credentials, and that the intruders had gained unauthorized access to earnings-related files of FA 2's publicly traded clients. Based on records obtained during the course of this investigation, it appears that the FA 2 compromise began as early as October 2017.

13. The table below sets forth some of the dates that the earnings-related files of particular companies were accessed and/or downloaded without authorization using the FA 2 employee's login credentials, together with the dates those companies publicly released their earnings and—to the extent reflected in the logs—which earnings-related files were accessed and/or downloaded.

UNAUTHORIZED ACCESS DATE	EARNINGS RELEASE DATE	COMPANY	FILES ACCESSED
02/05/2018	02/06/2018	Snap, Inc.	Form 8-K, Form 10-K, Form 10-Q, Exhibit_99_1.docx[4]
04/27/2018	05/01/2018	Nanometrics, Inc.	Exhibit 99.1.docx
04/27/2018	05/01/2018	McGrath Rentcorp.	Exhibit 99.1.docx
07/24/2018	07/25/2018	Grubhub, Inc.	Earnings Release.docx
07/24/2018	07/26/2018	Patterson-UTI Energy, Inc.	Exhibit99_1.docx
07/24/2018	07/26/2018	Ultra Clean Holdings, Inc.	Form 10-Q
07/24/2018	07/26/2018	CNH Industrial, N.V.	Form 6-K[5]
07/24/2018	07/25/2018	Getty Realty Corp.	Form 8-K
07/24/2018	07/26/2018	Essendant, Inc.	Earnings Release

[4] In quarterly and annual reports filed with the SEC, Exhibit 99.1 (or Exhibit 99-1) typically refers to an earnings-related press release.

[5] Form 6-K is a filing submitted to the SEC by certain foreign private issuers.

			Earnings Slides
07/24/2018	07/26/2018	The Nielsen Company	Exhibit 99.1.docx
10/12/2018	10/16/2018	Equity Bancshares, Inc.	Earnings_Release_Q3.docx
10/12/2018	10/17/2018	Brandywine Realty Trust	Exhibit 99.1docx
10/12/2018	10/19/2018	Mobile Mini, Inc.	Exhibit99_1.docx
10/24/2018	10/24/2018	Tesla, Inc.	Exhibit 99.1
10/26/2018	10/31/2018	SS&C Technologies	99.1.docx
10/29/2018			Form 8-K
10/31/2018			
11/04/2018	11/5/2018	Nevro Corp.	Exhibit99_1.docx
11/23/2018	11/28/2018	Box, Inc.	Exhibit 99.1
11/27/2018			
11/28/2018			
02/25/2019	02/26/2019	Tandem Diabetes Care, Inc.	2019_02_26ER.docx
02/26/2019			
05/20/2019	05/21/2019	Kohl's Corporation	Exhibit99_1.docx
07/22/2019	07/22/2019	HXL	Form 8-K
			Earnings Release.docx
07/23/2019	07/25/2019	AIMC	Form 8-K
			Exhibit_99.1.docx
			Exhibit_99.2.pptx
07/28/2019	07/29/2019	Medpace	Exhibit_99.1docx
10/17/2019	10/22/2019	Manhattan Associates, Inc.	Exhibit 99.1
10/22/2019			
10/31/2019	11/06/2019	Roku	Form 8-K
11/01/2019			Exhibit 99.1docx
11/04/2019			
11/05/2019			
11/06/2019			
11/05/2019	11/05/2019	Ichor	Form 8-K
			Exhibit 99_1.docx
11/05/2019	11/05/2019	Hubspot	Form 8-K
11/08/2019	11/12/2019	Datadog, Inc.	Exhibit 99.1.docx
11/25/2019	11/25/2019	Beacon Roofing Supply, Inc.	Ex-99.1.docx
05/18/2020	05/27/2020	Box, Inc.	Form 8-K
05/21/2020			Exhibit 99.1.docx
05/26/2020			
05/27/2020			

14. Based on my investigation, I am aware that, on at least several occasions, the intruders used computer servers located in the District of Massachusetts as part of their scheme. For example, the unauthorized access to Tesla's earnings-related files on or about October 24, 2018 originated from an internet protocol ("IP") address leased to a virtual private network ("VPN") provider and hosted at a data center located in Massachusetts.[6]

15. Based on my review of records obtained during the course of my investigation, I believe that the compromise of FA 2's network was related to the compromise of FA 1's network. Among other things, I am aware that, between on or about October 11, 2019 and November 4, 2019, at least three IP addresses associated with another VPN provider were used to gain unauthorized access to both FA 1's and FA 2's networks using compromised employee login credentials.

ERMAKOV and Intrusions at FA 2

16. Based on my review of records obtained from a U.S.-based technology company (the "Tech Company"), I have learned that on or about May 9, 2018, at 3:44 a.m. (ET), an account linked to ERMAKOV received an update for three native applications associated to the Tech Company. Records show that the May 9, 2018 application updates were associated to IP address 119.204.194.11 (the "119 IP Address").

---

[6] A VPN creates a secure, encrypted connection between a computer and a VPN server located elsewhere. A VPN can be used to hide the computer's IP address by replacing it with the VPN provider's IP address.

17. Based on my review of a log file from FA 2, I learned that on or about that same day, May 9, 2018, starting at 3:46 a.m. (ET)—approximately two minutes after ERMAKOV received application updates from the Tech Company—the FA 2 employee's compromised login credentials were used to gain unauthorized access to FA 2's system from the same 119 IP Address, and to view and/or download earnings-related files of four companies: Cytomx Therapeutics, Horizon Therapeutics, Puma Biotechnology, and Synaptics.[7] All four companies reported their quarterly earnings later that day.

IRZAK's and SLADKOV's Trading Related to the Intrusions at FA 1 and FA 2

18. IRZAK and SLADKOV both traded in the shares of most of the publicly traded FA 1 and FA 2 clients listed above around the time of the public announcements of the companies' financial performance, and I have reviewed records indicating that SLADKOV possessed earnings-related information of at least some of those companies prior to the time their earnings were announced.

19. The trading by IRZAK and SLADKOV was remarkably profitable. For example, between in or about August 2018 and November 2019, the IRZAK IB Account traded ahead of the earnings announcements of approximately 149 companies with a 66 percent success rate—meaning that IRZAK correctly anticipated whether a company's stock price would rise or fall following its earnings announcement approximately two-thirds of the time. Between in or about December 2019 and August 2020, the IRZAK IB Account traded ahead of earnings announcements of approximately 47 companies, generating profits of approximately $4.3

[7] FA 2's system was also accessed from the 119 IP Address on or about May 2, 2018 and May 3, 2018.

million. Since August 2020, approximately 169 companies in which IRZAK traded were clients of either FA 1 or FA 2. Several examples of IRZAK's timely trading are described below.

Snap, Inc.

20. On or about February 5, 2018, between 2:16 a.m. and 2:28 a.m. (ET), intruders used the FA 2 employee's login credentials to view and/or download drafts of earnings-related press releases and SEC filings of Snap, Inc. The intrusion took place one day before Snap reported its fourth quarter and full year 2017 financial results.

21. As part of the investigation, I have obtained a copy of a photograph that was in SLADKOV's possession. The photograph depicts a black Acer computer with a blue Band-Aid or sticker showing the logo of the Russian Olympic Committee (the "Russian Olympic Committee Sticker") covering the computer's camera. The document on the computer screen appears to be part of the press release announcing Snap's fourth quarter and full year 2017 financial results. The timestamp of the photograph is February 6, 2018 at 8:13 a.m. (ET). Based on my review of the SEC EDGAR filing system, I am aware that Snap's Form 8-K reporting the company's fourth quarter and full year 2017 financial results was not accepted for filing until 4:20 p.m. (ET) that same day—more than eight hours after the timestamp on SLADKOV's photograph. A copy of the press release displayed on the computer screen was appended to Snap's Form 8-K as Exhibit 99.1.

22. Snap's share price increased significantly following the public announcement of its better-than-expected financial results. I have reviewed other photographs in SLADKOV's possession showing what appears to be the BCS trading application displaying the sale of approximately 3,000 Snap shares in one of the SLADKOV BCS Accounts following the

announcement. The top portion of one of the photographs lists SLADKOV's full name in Cyrillic and an IP address at the bottom that is associated with BCS.

Nanometrics and McGrath RentCorp.

23. On or about April 27, 2018, intruders gained unauthorized access to earnings-related filings on FA 2's network for Nanometrics, Inc. and McGrath Rentcorp. Both companies reported their first quarter 2018 financial results four days later, after the stock market closed on or about May 1, 2018.

24. I have obtained a copy of a May 2, 2018 photograph that was in SLADKOV's possession showing a computer screen—with the Russian Olympic Committee Sticker covering the computer's camera—displaying what I believe to be trading activity in both Nanometrics and McGrath using the BCS stock trading application. The photograph shows SLADKOV's name in Cyrillic and his BCS user identification number on the screen.

Seven Companies

25. On or about July 24, 2018, intruders leveraged the FA 2 employee's compromised login credentials to gain access to 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 seven companies reported their quarterly earnings over the next two days.

26. I have reviewed another SLADKOV photograph dated July 24, 2018, at 2:05 p.m. (ET). The photograph appears to show IRZAK sitting at a brown table with two computers, note pads, a blue pen, and a smartphone, among other items. One of the computers is the black Acer laptop with the Russian Olympic Committee Sticker covering the computer camera. A second

photo, taken approximately two minutes later, shows SLADKOV facing the camera and IRZAK staring at an Apple iMac computer next to the Acer laptop. Facebook location data[8] indicates that IRZAK was at or in close proximity to SLADKOV's St. Petersburg, Russia residence at approximately the time the photo was taken.[9]

27. Another SLADKOV photograph, dated July 25, 2018, appears to display trading activity in one of the SLADKOV BCS Accounts in each of the seven companies whose financial information was accessed without authorization the prior day.

Equity Bancshares, Brandywine Realty, and Mobile Mini

28. On or about October 12, 2018, compromised login credentials were used to gain access to FA 2's network to view earnings-related files of Equity Bancshares, Brandywine Realty, and Mobile Mini.

29. I have reviewed a photograph in SLADKOV's possession dated October 14, 2018, depicting a handwritten note resting on what appears to be a brown table. The note shows the stock symbols for Equity Bancshares, Brandywine Realty, and Mobile Mini, with a rectangle drawn around the three symbols and the word "short" handwritten in blue ink in English.

---

[8] Facebook records date, time, latitude, and longitude location data for the Facebook account holder's device linked to the Facebook account.

[9] IRZAK lives approximately six miles from SLADKOV in St. Petersburg, Russia.

30. On or about October 16, 2018, IRZAK sold short[10] shares of Equity Bancshares in the IRZAK IB Account. Equity Bancshares reported its third quarter financial results later that same day, after the market closed.

31. On or about October 17, 2018, IRZAK sold short shares of Brandywine Realty. Brandywine Realty reported its third quarter financial results later that day, after the market closed. Mobile Mini reported its third quarter financial results on or about October 19, 2018 before the market opened.

Tesla, Inc.

32. On or about October 24, 2018, approximately two hours after intruders accessed FA 2's network to view Tesla's earnings-related information, IRZAK purchased approximately 200 shares of Tesla in the IRZAK IB Account. After the close of the market that day, Tesla reported positive third quarter financial results. IRZAK sold all the Tesla shares for a profit of approximately $3,500.

SSNC

33. I have reviewed a photograph in SLADKOV's possession dated October 31, 2018, at 2:42 p.m. (ET), depicting part of what appears to be a press release announcing third quarter 2018 financial results for SSNC. SSNC did not report its earnings results until after the market closed that day.

---

[10] In general, "selling short" or "shorting" refers to selling a security with plans to buy it back (or "cover" the position) later. Shorting is a strategy that is often used when investors anticipate that the price of a security will fall prior to the expiration of the short position.

Nevro

34. On or about November 4, 2018, intruders accessed FA 2's network to view Nevro's earnings-related information. The next day, IRZAK sold short approximately 1,009 Nevro shares. After the close of the market, Nevro announced third quarter 2018 financial results that missed consensus estimates.

35. IRZAK covered his short positions the following day, realizing an overnight profit of approximately $6,800.

Box – November 2018

36. On and before November 28, 2018, intruders downloaded Box's draft earnings press release from FA 2's network. That same day, IRZAK purchased approximately 3,800 shares of Box in the IRZAK IB Account. After the close of the market, Box reported third quarter 2018 financial results that exceeded market estimates. IRZAK sold his 3,800 Box shares for a profit of approximately $3,400.

Tandem Diabetes Care

37. Based on review of a log file from FA 2, I learned that on or about February 25, 2019 and February 26, 2019, the FA 2 employee's compromised login credentials were used to gain unauthorized access to earnings-related files of Tandem.

38. Based on review of SLADKOV's BCS trading activity, I learned that between February 25 and February 26, 2019, SLADKOV purchased 33,000 shares of Tandem in one of the SLADKOV BCS Accounts.

39. Likewise, on or about February 26, 2019, IRZAK purchased 2,000 shares of Tandem in the IRZAK IB Account. After the close of the market, Tandem announced its fourth

quarter and full-year 2018 financial results. IRZAK subsequently sold his Tandem shares for a profit of approximately $10,000. SLADKOV sold his Tandem shares for a profit of approximately $350,000.

Kohl's

40. On or about May 20, 2019, between 8:28 a.m. and 8:30 a.m. (ET), FA 2's system was accessed without authorization to view Kohl's earnings-related information.

41. Beginning at 9:50 a.m. (ET) that same day, SLADKOV opened short positions in one of the SLADKOV BCS Accounts in 60,000 Kohl's shares.

42. Beginning at 10:01 a.m. (ET), IRZAK opened short positions in the IRZAK IB Account in 7,000 Kohl's shares. IRZAK also opened short positions in another 4,000 Kohl's shares in the IRZAK Saxo Account.[11] I have reviewed communications between and among IRZAK, SLADKOV, and a Saxo Bank representative which indicate that IRZAK and SLADKOV jointly opened the Saxo account just over one year earlier.[12]

43. On or about the following day, before the stock market opened, Kohl's publicly announced financial results that fell below analyst expectations, prompting its share price to fall.

---

[11] The trading by IRZAK in the Saxo account utilized contracts for difference ("CFDs"), which allow traders to participate in the price movements of securities without actually owning those securities. For example, a trader can purchase a long or short position in a CFD that tracks the price of the stock of a publicly traded U.S. company. The value of the CFD will increase or decrease depending on whether the price of the underlying stock increases or decreases.

[12] On or about March 12, 2018, IRZAK received an e-mail from a Saxo Bank representative regarding certain bank policies. IRZAK subsequently forwarded the Saxo e-mail to SLADKOV. The next day, IRZAK sent the Saxo representative an e-mail in Cyrillic that reads, in substance: "Good afternoon, Sergey! Thanks for the info. My partner and I decided to open a trial account for a small amount, try services, etc. I want to deposit 20,000 USD in my name. How do we proceed? Michael."

44. Beginning within minutes of the Kohl's announcement, IRZAK covered his short positions, earning an overnight profit of approximately $41,000 in the IRZAK IB Account and approximately $29,000 in the IRZAK Saxo Account. SLADKOV also covered his short positions, earning an overnight profit of approximately $400,000. That same day, SLADKOV and ERMAKOV shared screenshots showing Kohl's share price.

Manhattan Associates, Inc.

45. On or about October 22, 2019, between 3:45 p.m. and 3:52 p.m. (ET), hours after the FA 2 employee's login credentials were used to access earnings-related information of Manhattan Associates, IRZAK purchased approximately 5,000 shares of Manhattan Associates in the IRZAK IB Account.

46. Manhattan Associates reported record third quarter financial results approximately 20 minutes later, after the close of the market, prompting its share price to increase.

47. IRZAK promptly sold the shares of Manhattan Associates he had just purchased, earning a profit of approximately $23,000.

Datadog, Inc.

48. On or about November 11, 2019—approximately three days after the FA 2 employee's login credentials were used to access earnings-related information of Datadog—IRZAK purchased approximately 6,000 shares of Datadog in the IRZAK IB Account. IRZAK purchased approximately 24,000 additional shares the following day.

49. On the same day, November 11, 2019, IRZAK also purchased approximately 3,000 shares of Datadog in the IRZAK Millennium Account.

50. After the stock market closed on November 12, 2019, Datadog announced positive third quarter financial results, prompting its share price to increase.

51. IRZAK promptly sold all of the shares of Datadog he had just acquired, earning a profit of approximately $120,000 in the IRZAK IB Account and approximately $19,500 in the IRZAK Millennium Account.

Beacon Roofing Supply, Inc.

52. On or about November 25, 2019, just hours after Beacon's earnings press release was accessed by way of the FA 2 employee's compromised login credentials, IRZAK sold short approximately 15,000 shares of Beacon Roofing Supply in the IRZAK IB Account.

53. That same day, after the close of the market, Beacon reported fourth quarter financial results that fell short of analysts' consensus projections. Following the announcement, the price of Beacon's shares declined.

54. IRZAK covered most of his short position the following morning, earning a profit of approximately $35,000.

55. Based on records I have reviewed, SLADKOV traded Manhattan Associates, Datadog, and Beacon in parallel with IRZAK in one of the SLADKOV BCS Accounts, earning approximately $700,000 in combined profits.

IBM

56. As noted above, on or about January 21, 2020, between 8:58 a.m. and 9:34 a.m. (ET), an FA 1 employee's compromised login credentials were leveraged to access IBM's draft earnings press release.

57. That same day, beginning at 10:40 a.m. (ET), IRZAK purchased approximately 5,000 shares of IBM in the IRZAK IB Account.

58. After the close of the market, IBM reported favorable fourth quarter and full year 2019 earnings results, prompting its share price to increase.

59. IRZAK sold all the IBM shares he had just acquired the following morning, earning a profit of approximately $34,000.

Avnet, Inc.

60. On or about January 23, 2020, two days after intruders accessed earnings-related information of Avnet at FA 1, IRZAK sold short approximately 12,000 shares of Avnet in the IRZAK IB Account.

61. After the market closed that day, Avnet reported its second quarter 2020 financial earnings that fell short of analysts' estimates.

Box – May 2020

62. On or about May 27, 2020, and on various dates before then, intruders accessed FA 2's network and viewed unreleased drafts of the press release announcing Box's financial results for the first quarter of fiscal 2021.

63. Later that same day, IRZAK purchased approximately 20,000 Box shares in the IRZAK IB Account.

64. At approximately 3:47 p.m. (ET)—shortly before the close of the market—SLADKOV shared a screenshot with a BCS representative showing what appears to be the BCS trading application displaying trading activity in Box. The top portion of the screenshot lists SLADKOV's name in English.

65. After the close of the market, Box reported quarterly earnings and revenue that exceeded Wall Street estimates.

66. IRZAK promptly sold all of his Box shares, earning a profit of approximately $16,000.

Trading By ERMAKOV and KLYUSHIN in Companies Affected by the Intrusions

67. ERMAKOV and KLYUSHIN also traded profitably in shares of companies whose earnings-related information was improperly accessed.[13]

68. I have reviewed records indicating that ERMAKOV has SaxoTraderGO, a mobile trading app for Saxo Bank clients, on his smartphone. The records include an image of a

---

[13] I have reviewed communications in which KLYUSHIN and ERMAKOV discussed using the proceeds of their trading to purchase real estate. For example, on or about June 30, 2020, ERMAKOV sent KLYUSHIN a brochure for a residential property located in Moscow, Russia. ERMAKOV and KLYUSHIN then engaged in the following message conversation in which they discussed "earning" money to purchase the property by "turn[ing] on the computer" instead of by working:

ERMAKOV:	324
ERMAKOV:	Final price
KLYUSHIN:	if there's money it could be bought
KLYUSHIN:	i'm not ready
ERMAKOV:	Me too for now
KLYUSHIN:	key word for now [three smiles]
KLYUSHIN:	apartment is cool
ERMAKOV:	[winking face emoji]
KLYUSHIN:	*we'll earn and then we can buy [it]*
ERMAKOV:	*Need to go to work then [smile]*
KLYUSHIN:	*no need to*
KLYUSHIN:	*just turn on the computer*
KLYUSHIN:	*[three smiles]*
KLYUSHIN:	and give it a little thought [three smiles]
ERMAKOV:	I already thought yesterday
ERMAKOV:	Today I will think some more [smile]
KLYUSHIN:	[four loudly crying face emojis]

"Trading" screen dated January 23, 2020 from the SaxoTraderGO app on ERMAKOV's smartphone. The screen shows a "Trade Ticket" order for Avnet and a Saxo trading account number that I know based on review of wire transfer information is associated to KLYUSHIN. The Trade Ticket shows a "Net position" of "-36k" (or negative 36,000) prior to the close of the market on January 23, 2020, and an available balance of approximately $4.5 million. Based on my review of this image and my knowledge of this investigation, I believe that ERMAKOV has access to KLYUSHIN's Saxo trading account, and that he shorted Avnet using CFDs on or about January 23, 2020.[14] As noted above, that was two days after intruders accessed FA 1's system to view earnings-related information of Avnet, and the same day that IRZAK sold short shares of Avnet.

69. KLYUSHIN also used at least one account at Otkritie Broker, Ltd. ("OTK Broker"), a Russia-based bank that provides brokerage services, to trade in shares of companies whose earnings-related information the intruders accessed.[15] The activity included trading in the

---

(emphasis added).

[14] For example, on or about February 21, 2020, KLYUSHIN and ERMAKOV had the following message exchange regarding a Saxo account:

KLYUSHIN:	Let me help you with saxo
KLYUSHIN:	if you need [me], otherwise i'm sitting here with nothing to do
ERMAKOV:	I [can do it] myself
KLYUSHIN:	ok
ERMAKOV:	Thanks

[15] In connection with his purchase of a yacht, KLYUSHIN provided income documentation that included OTK brokerage account records for the period between July 17, 2018 and November 29, 2018.

shares of 52 companies, including Snap, Tesla, Kohl's, SSNC, and Box. All but one of the companies used FA 2 as their filing agent.

70. As noted above, intruders downloaded Box's draft earnings press release from FA 2's system on and before November 28, 2018, and IRZAK executed timely trades in that company's stock the same day, just before Box released its earnings report to the public. Five days later, on or about December 3, 2018, KLYUSHIN and ERMAKOV engaged in the following message conversation about closing out a position in "box":[16]

ERMAKOV:	hi
ERMAKOV:	I wont be able to call you back
ERMAKOV:	forgot [my] telephone at work
KLYUSHIN:	Hi. I wanted to see how your trades are going [smile] it's that Kolya's away on vacation[17]
ERMAKOV:	our assets have grown
ERMAKOV:	some I will close today
ERMAKOV:	we will wait a bit more on the other ones
ERMAKOV:	it's painful they have fallen badly, we need to wait a bit more
KLYUSHIN:	ok
ERMAKOV:	*I will close box today* [emphasis added]
KLYUSHIN:	thanks for the info [smile]

[16] Unless otherwise noted, all message conversations referenced herein are draft translations from Cyrillic.

[17] I am aware that "Kolya" is short for Nikolay or Nikolai. Based on my knowledge of this investigation and review of records, I believe that Kolya is a reference to RUMIANTCEV.

ERMAKOV: you're welcome, sorry it wasn't timely

ERMAKOV: i am fighting with two [redacted]!

KLYUSHIN: you're crazy [two smiles] you are always super timely

[three smiles]

ERMAKOV: thanks [three smiles]

KLYUSHIN, ERMAKOV, and RUMIANTCEV Managed Others' Trading Accounts in Furtherance of the Scheme

71. I also have probable cause to believe that KLYUSHIN, ERMAKOV, and RUMIANTCEV have engaged in profitable trading on behalf of other individuals while in possession of MNPI that was accessed without authorization from FA 1's and FA 2's system using compromised login credentials. As previously noted, all three men are listed as employees of M-13, a purported IT company based in Moscow, Russia. I further have probable cause to believe that KLYUSHIN, ERMAKOV, and RUMIANTCEV received a portion of the illicit trading profits they generated for their clients.

Trading on Behalf of Alexander Borodaev and Boris Varshavskiy

72. On or about October 24, 2018, at 1:28 p.m. (ET), hours after intruders accessed FA 2's system to view Tesla's draft earnings press release, and before Tesla had publicly announced its earnings, KLYUSHIN sent the following message to two individuals, Alexander Borodaev (also known as "Sasha") and Boris Varshavskiy:[18]

KLYUSHIN: Pay attention to shares of Tesla now and tomorrow after 16:30 and on how much they go up

[18] As noted above, IRZAK also engaged in timely trading in Tesla shares in the IRZAK IB Account just before Tesla reported positive financial results for the third quarter of 2018.

73. At 4:18 p.m. (ET), KLYUSHIN sent Borodaev and Varshavskiy a smartphone screenshot showing Tesla's stock price at $288.50, down 1.92 percent. One minute later, KLYUSHIN sent the following message to them:

KLYUSHIN:	It was 288 but after the close it was already 308, and tomorrow will most likely hit 330 that's 10 [percent]. And with a shoulder 2-3 times its almost 25 [percent]. But such deals don't happen often in a quarter.

74. On or about February 7, 2019, between 9:52 p.m. and 9:59 p.m., KLYUSHIN engaged in the following group chat conversation with Borodaev and Varshavskiy:

KLYUSHIN:	preliminary report on stock trading for now all is not as we would have wished. Boris $173 861 Alexander $155 821. The end results we will figure in the end of February and we can pay the 13 [percent] of added tax value <u>and we split the remainder</u>. [emphasis added]
KLYUSHIN:	Boris was more lucky he has added 34 [percent] while Alexander had only 15 [percent]
KLYUSHIN:	But we are working and hope to rectify the situation
Borodaev:	Good result! Who pays the 13 [percent], we or the broker?
Varshavskiy:	Vlad [face with tears of joy emoji] !
KLYUSHIN:	Who pays I don't know. When we finish the quarter I'll clear it up and tell [you]. But I think the first profits we can withdraw in March and leave 1 million nominal with Sasha and 500k with Boris. Or however it suits you.

75. Based on my training and experience and my knowledge of this investigation, I believe KLYUSHIN was relaying to Borodaev and Varshavskiy their profits on the trades he had conducted on their behalf. I further believe that his reference to "split[ting] the remainder" after paying taxes was to the portion of the profit from that trading that he would retain.

76. On or about March 11, 2019, at 10:41 a.m., KLYUSHIN sent the following message to Borodaev and Varshavskiy:

KLYUSHIN: Good morning! I have returned, am rested and ready to work [smile]. I congratulate Boris on his super result earning $632k in 4 months, and Alexander a little worse than that at $461k. Also the brokers added a new function and one can watch their portfolio online, below I am sending you a login and password, and you can check it any time. There will be no more trading until April 15 so you may withdraw extra funds.

KLYUSHIN then provided Borodaev and Varshavskiy with the login name and password to their OTK Broker trading accounts in their individual names.

77. On or about May 25, 2019, KLYUSHIN and ERMAKOV engaged in the following message conversation:

KLYUSHIN: [I] counted for Boris [and he's got] 198 [percent] profitability starting November 1 18 [2018] ending May 25, 2019

ERMAKOV: And for Sasha [Alexander Borodaev]?[19]

KLYUSHIN: one second

KLYUSHIN: 69.3 [percent] [three faces with tears of joy emoji]

KLYUSHIN: Boris earned $989k on 500k

KLYUSHIN: Sasha $693k on 1 million [smile]

KLYUSHIN: They don't even ask why so anymore [smile]

KLYUSHIN: I said strategies are different and we are looking closely for now [smile]

[19] On or about November 19, 2020, ERMAKOV and Borodaev exchanged multiple messages.

ERMAKOV: [thumbs up emoji] [three faces with tears of joy emoji]

78. On or about June 13, 2019, at 2:58 p.m., KLYUSHIN messaged ERMAKOV the following: "Kolya's [RUMIANTCEV] assets have grown [three smiles]." At 5:23 p.m., ERMAKOV responded: "Yes [smile]."

79. On or about July 25, 2019, KLYUSHIN sent Borodaev and Varshavskiy statements of the trading activity in their OTK Broker accounts. The documents indicate that during the three-day period between July 22, 2019 and July 24, 2019, Borodaev's OTK Broker account traded in shares of eight companies. Four of those companies—3M Company ("3M"), Amphenol Corporation, CoreSite Realty Corp, and Steel Dynamics—used FA 1 as their filing agent, while the remaining four companies—AIMC, Tesla, Snap, and Hexcel Corporation—used FA 2 as their filing agent. All eight companies reported their second quarter 2019 financial results between July 22, 2019 and July 25, 2019.

80. Over the same three-day period, Varshavskiy's OTK Broker account traded in parallel with Borodaev's OTK Broker Account in five of the eight companies: 3M, Steel Dynamics, Tesla, Snap, and Hexcel.

81. IRZAK and SLADKOV also traded in parallel with Varshavskiy's and Borodaev's OTK Broker accounts in seven of the eight companies, in the IRZAK IB Account and one of the SLADKOV BCS Accounts. IRZAK earned approximately $160,500 from his trades, while SLADKOV made approximately $1.9 million.

82. Based on information provided by FA 2, I am aware that during the three-week period leading up to that trading, the FA 2 employee's login credentials were used without authorization to access earnings-related files associated with AIMC, Hexcel, Tesla, and Snap.

83. Likewise, according to a statement summarizing trading activity in Borodaev's OTK Broker account during the four-day period between July 26, 2019 and July 30, 2019, the account traded in shares of six companies—Proofpoint, Paycom, SSNC, Grubhub, Medpace, and Martin Marietta—all of which used FA 2 as their filing agent. And according to a statement summarizing trading activity in Varshavskiy's OTK Broker account for the same period, the account traded in parallel in all of those companies except Grubhub. All six companies reported their second quarter 2019 financial results between July 25, 2019 and July 30, 2019.

84. IRZAK traded in parallel with Varshavskiy's and Borodaev's OTK Broker accounts in all six companies, while SLADKOV traded in parallel in five of the companies in one of the SLADKOV BCS Accounts.[20] IRZAK earned approximately $98,000 from his trades while SLADKOV earned approximately $1.2 million.

85. Based on information provided by FA 2, I am aware that between on or about July 23, 2019 and July 29, 2019, the FA 2 employee's login credentials were used to access earnings-related files of all six companies.

86. On or about November 7, 2019, KLYUSHIN sent Borodaev and Varshavskiy a screenshot showing trading in Borodaev's Saxo brokerage account in Ichor Holdings, Hubspot, and Roku. As noted above, all three companies used FA 2 as their filing agent, and intruders accessed FA 2's system to view their earnings-related files shortly before public announcements of their earnings on November 5 and 6, 2019.

Trading on Behalf of Sergey Uryadov

---

[20] IRZAK also traded Paycom in the IRZAK Millennium Account.

87. On or about June 9, 2020, KLYUSHIN sent RUMIANTCEV several photographs of Varshavskiy and others on a small private jet, including a passenger identified as Sergey Uryadov. KLYUSHIN and RUMIANTCEV then engaged in the following message conversation in which they referred to Varshavskiy and Uryadov as their "investors":[21]

KLYUSHIN:	And here is the London with our investors [three smiles]
KLYUSHIN:	Recognize all of them? [smile]
RUMIANTCEV:	Varshavskiy and Uryadov
KLYUSHIN:	Exactly
RUMIANTCEV:	Is Varshavskiy still works with us on trading?
RUMIANTCEV:	Or on some other projects
KLYUSHIN:	Of course, they split everything 50/50 with Borodaev
KLYUSHIN:	The 50 [percent] that Sasha [Alexander Borodaev] gives to Boris
RUMIANTCEV:	Oh, just decided to put it all in the name of one person, got it. Do we leave their OBL accounts or close them?
KLYUSHIN:	Leave them

[21] I am aware based on documents and communications I have reviewed that KLYUSHIN, ERMAKOV, Varshavskiy, and Uryadov are friendly with one another and travel together. For example, I have reviewed photographs in KLYUSHIN's possession of Varshavskiy and Uryadov standing across the street from the headquarters of New Scotland Yard, in London, England, and of himself with Uryadov in front of the United Kingdom Ministry of Defense building. KLYUSHIN has also shared photographs of ERMAKOV with Varshavskiy.

88. Based on my review of records obtained during the course of my investigation, I believe that when RUMIANTCEV asked KLYUSHIN about "their OBL accounts," he was referring to Varshavskiy's, Uryadov's, and Borodaev's OTK accounts.[22]

89. According to information obtained from FINRA, between on or about October 16, 2019, and November 7, 2019, a client account at OTK Broker (the "OTK Client Account") profitably traded ahead of quarterly earnings announcements of approximately 27 companies, realizing overall combined profits of approximately $7 million in less than 30 days. Based on my training and experience and my knowledge of this investigation, I believe the OTK Client Account may be an omnibus account representing multiple OTK Broker clients.

90. Of the 27 companies, approximately 16 used FA 2 as their filing agent, and the remaining 11 used FA 1 as their filing agent.[23] Based on information provided by FA 2, I am aware that between on or about October 17, 2019 and November 6, 2019, the FA 2 employee's login credentials were used to gain unauthorized access to earnings-related files of all 16 FA 2

---

[22] I have also reviewed communications in which KLYUSHIN and Uryadov discussed the proceeds from trading. On or about June 13, 2019, KLYUSHIN sent Uryadov a picture of what appears to be a leather carry bag and then engaged in the following message conversation:

KLYUSHIN:	I had a good [profitable] day today
KLYUSHIN:	We made 1.2 million dollars on [trades] in the stock exchange and passed on 70 in suitcase [smile]
KLYUSHIN:	I did my deed
Uryadov:	You're the man
Uryadov:	I'm proud of you
KLYUSHIN:	Thank you [smile]

[23] In or about October 2018, ERMAKOV installed the OTK Broker trading app on his smartphone. IRZAK and SLADKOV traded in parallel with the OTK Client Account on several occasions, including in shares of IBM, Avnet, Snap, Tesla, Skechers, and Manhattan Associates. These companies all used either FA 1 or FA 2 as their filing agents.

client companies. Approximately 11 of those 16 companies were accessed from the IP address 64.42.179.59 (the "64 IP Address"), which was one of the IP addresses that had been collected by FA 1 during the intrusion investigation as one of the indicators of compromise ("IOCs").[24]

91. I have reviewed a copy of Uryadov's OTK Broker account statement (the "Uryadov OTK Broker Account") in KLYUSHIN's possession for "Reporting date and time" of October 28, 2019. The statement indicates that between October 23, 2019 and October 25, 2019, the Uryadov OTK Broker Account traded in parallel with the OTK Client Account in Six Flags, 3M, Manhattan Associates, Microsoft, Skechers, Tesla, Proofpoint, and Universal Health surrounding their earnings. Six Flags and 3M used FA 1 as their filing agent while the rest used FA 2 as their filing agent.

92. Based on my review of a log file from FA 2, I am aware that between on or about October 17, 2019 and October 24, 2019, the FA 2 employee credentials were used to gain unauthorized access to earnings-related files of Manhattan Associates, Microsoft, Skechers, Tesla, Proofpoint, and Universal Health.

93. I have reviewed a smartphone screenshot in KLYUSHIN's possession, dated on or about July 27, 2020, displaying an e-mail to KLYUSHIN from RUMIANTCEV's M-13 e-mail account (NR[@]M13[.]ru). In the e-mail, which has the subject "Report on June-July 2020," RUMIANTCEV indicated, in substance, that he was sending trading results from the prior day, and the "profit for BURL" for the prior quarter. Based on my knowledge of this

[24] Indicators of compromise ("IOCs") serve as forensic evidence/artifacts of potential intrusions on a network or a host system. IOCs enable system administrators or cyber security experts to detect intrusion attempts or other malicious activities.

investigation, I believe that BURL is a reference to Burlington Stores, Inc., which used FA 2 as its filing agent. Based on review of a log file from FA 2, I am aware that on or about May 11, May 18, May 21, May 26, and May 27, 2020, intruders used the 64 IP Address to gain unauthorized access to earnings-related information of Burlington Stores.[25]

94. The RUMIANTCEV e-mail contains a partial table with the columns broken down by "Accounts;" "Changes to Portfolio for June 1 to July 24, 2020;" "Start-up Capital;" "Value on July 24, 2020 at 23:00;" "Customer;" and "Share;" among others. The "Accounts" column lists what appear to be trading accounts labeled as "VK_SAXO," broken down further in the "Customer" column as "VKS1," "VKS2," and "VKS3". Based on the initials associated with the accounts, as well as the fact that I have reviewed records of multiple wire transfers from KLYUSHIN's Russian Standard Bank account to Saxo Bank, I believe that KLYUSHIN may have additional accounts with Saxo.[26]

95. The Accounts column also lists what I believe to be trading accounts bearing labels that included the following initials: "AB_SAXO," "USS_SAXO," "NR," "M13," "VK5," and "VK_BCS". Based on the initials and my knowledge of this investigation, I believe the "NR" trading account is RUMIANTCEV's trading account, that "AB_SAXO" and

---

[25] On or about May 21, May 26, and May 27, 2020, SLADKOV and a BCS representative shared a screenshot of a computer screen of what appears to be SLADKOV's BCS trading app. The screenshot shows trading activity in BURL.

[26] On or about January 17, 2020, approximately $505,367.59 was transferred from KLYUSHIN's Russian Standard Bank account to his Saxo account "FOR PARTICIPATION IN TRADING."

"USS_SAXO" are references to Borodaev's and Uryadov's Saxo trading accounts,[27] and that the "VK_BCS," account broken down further in the "Customer" column as "BCS1" and "BCS2" are KLYUSHIN's trading accounts with BCS Prime Brokerage Limited (UK) ("the KLYUSHIN BCS Prime Account").[28] Based on my knowledge of this investigation and my review of the e-mail noted above, I believe that the trading accounts labeled in the table are managed by KLYUSHIN and RUMIANTCEV.[29]

96. Additionally, KLYUSHIN has an image of another table dated August 7, 2019, at 6:51 p.m., with an "Accounts" column that lists what I believe to be trading accounts labeled with KLYUSHINS's initials "VK," "VK2," VK3," "VK4," "VK5," "VK_SAXO," Varshavskiy's and Borodaev's initials "BV" and "AB," "SA," Uryadov's initials "USS," "ASF," RUMIANTCEV's initials "NR," and "M13." The table lists the combined amount on "7.08"—which I believe to be a reference to August 7, 2019—as approximately $18.6 million, and the combined amount earned for the quarter as approximately $7.7 million.

97. I have reviewed a smartphone screenshot in KLYUSHIN's possession, dated September 17, 2020, displaying an e-mail from RUMIANTCEV to KLYUSHIN. The subject of the e-mail reads, in substance: "Fixed profit at the end of 3rd quarter of 2020 for brokerage

---

[27] I am aware that Uryadov's full name is Sergey Sergeyevich Uryadov and one of his e-mail accounts is USS[@][redacted][.]su.

[28] I am aware that on or about January 29, 2020, approximately $3.3 million was transferred from KLYUSHIN's Russian Standard Bank to the KLYUSHIN BCS Prime Account.

[29] I have reviewed smartphone screenshot images in KLYUSHIN's possession displaying the KLYUSHIN Saxo Account and Borodaev's and Uryadov's Saxo trading accounts.

account of Alexander Borodaev (draft)." The text of the e-mail reads, in substance: "Greetings. The company M 13 has concluded 3rd quarter 2020 and plans to fix profits according to trade results details provided in the table." The table shows the investment capital as approximately $10 million and the profit on September 17, 2020 as approximately $1.3 million, and indicates that M-13 would receive 60 percent of Borodaev's net profit from the trading.

98. I have also reviewed a smartphone screenshot in KLYUSHIN's possession dated on or about September 18, 2020, displaying an e-mail from RUMIANTCEV to KLYUSHIN with the subject: "RE: Fixed profit at the end of 3rd quarter of 2020 for the brokerage account of Sergey Uryadov (draft)." The text of the e-mail reads, in substance: "Greetings. The company M 13 has concluded 3rd quarter 2020 and plans to fix profits according to trade results. Details provided in the table." The table shows the investment capital as approximately $5 million and the profit on September 17, 2020 as approximately $1,125,273. The table shows that M-13 would receive 60 percent of Uryadov's net profit from trading.

The FA 1 and FA 2 Intruders' Connection to M-13, KLYUSHIN, ERMAKOV, and RUMIANTCEV

99. According to FA 1, the following domains—all hosted by Vultr Holdings Corporation—were used as part of the intrusion into FA 1's network:

www.developingcloud[.]info - ("Vultr Domain 1")

financecloudapi[.]com - ("Vultr Domain 2")

cloudapifinance[.]info - ("Vultr Domain 3")

appfinreport[.]info - ("Vultr Domain 4")

finwallinform[.]info - ("Vultr Domain 5")

www.finshopland[.]me - ("Vultr Domain 6")

www.shopservice[.]live - ("Vultr Domain 7")

(collectively, "the Vultr Domains")

100. For instance, according to FA 1, forensic artifacts revealed that on or about January 17, 2020, Vultr Domain 1 connected with one of the computers on FA 1's network. The connection appears to have occurred via malware previously installed on FA 1's network to create a remote "backdoor" to FA 1's network.[30]

101. Forensic artifacts also revealed that Vultr Domain 6 and Vultr Domain 7—which were registered with the domain registrar Namecheap on or about May 15, 2019—were found encoded in a PowerShell command in one of FA 1's computers.[31] The PowerShell command containing these domains appears to have been executed on FA 1's network for the purpose of credential harvesting and/or to maintain a persistent presence in FA 1's network environment.

102. Records obtained from Vultr reveal that the Vultr Domains are associated with a Sweden-based hosting company, 99Stack.

103. Records obtained from 99Stack reveal that the IP addresses that pointed to the Vultr Domains used in the FA 1 intrusion were assigned to a user account created in or about August 2018 in the name of "Andrea Neumann" with an associated e-mail address of neumann[@]dr.com (the "Neumann Account").

---

[30] A backdoor is a means to access a computer system or network that bypasses the system's customary security mechanisms.

[31] PowerShell is a user interface, initially developed by Microsoft for the purposes of task automation and configuration management, that gives its users access to various services of an operating system. PowerShell allows users to automate tasks by creating scripts and combining multiple commands.

104. Records from 99Stack also reveal that the Neumann Account was registered from the IP address 89.238.166.235 (the "First 89 IP Address").

105. According to information obtained from FA 1, the First 89 IP Address was one of the IOCs collected during FA 1's intrusion investigation. Likewise, according to information obtained from FA 2, the First 89 IP Address was among those used in October and November 2019 to gain unauthorized access to earnings-related information on FA 2's system concerning Sleep Number Corp., Tesla, Microsoft, and Tandem.

106. E-mails obtained from the Neumann Account pursuant to a Court-authorized search warrant indicate that the account was used to register domain names with Namecheap. Namecheap and BitPay account records indicate that a Bitcoin wallet was used to pay for Neumann's Namecheap account in or about August 2018 (the "Neumann BTC Wallet").

107. Based on my review of Bitcoin transactions associated with the Neumann BTC Wallet, I learned that on or about October 29, 2018, at 6:27 a.m. (ET), the Neumann BTC Wallet sent .00516365 in Bitcoin (approximately $33.02) to fund another Bitcoin wallet (the "Second BTC Wallet").

108. On or about November 22, 2018, at 4:34 a.m. (ET), the Second BTC Wallet sent .0035 in Bitcoin (approximately $15.87) to fund a third Bitcoin wallet (the "Third BTC Wallet"). Approximately two hours later, at 6:43 a.m. (ET), the Third BTC Wallet sent .000452 (approximately $2.02) to BitPay to fund a Namecheap account (the "November 22 BitPay Transaction").

109. Based on my training and experience investigating cyber and financial matters and records obtained in the investigation to date, the use of chains of Bitcoin addresses to fund

transactions is consistent with those Bitcoin addresses being controlled by a single accountholder who is attempting to obfuscate the source of the Bitcoin. In other words, I believe that the same individual controls the Neumann BTC Wallet, the Second BTC Wallet, the Third BTC Wallet, and the Namecheap account for which the November 22 BitPay Transaction was made.

110. Based on my review of BitPay and Namecheap records, I learned that the November 22 BitPay Transaction noted above is linked to a BitPay user with the e-mail address Wan-Connie909[@]inbox[.]lv (the "Wan E-Mail Account") who, according to BitPay, viewed the November 22 BitPay Transaction invoice from IP address 89.107.124.42 (the "Second 89 IP Address"). Namecheap account records associated to the Wan E-Mail Account also shows login activity from the Second 89 IP Address on or about November 22, 2018, at 6:12 a.m. (ET).

89.107.124.42 - The M-13 IP Address

111. Based on publicly available information and records gathered during the course of this investigation, I am aware that M-13's web address is hxxp://www[.]M13[.]su. Based on my review of historical domain records and my review of records gathered during the course of this investigation, I learned that a Google account and a Hotmail account that are associated to RUMIANTCEV are listed in the registrant section of M-13's domain record.

112. Based on open-source research, I am aware that the Second 89 IP Address points to canmos[.]ru ("Canmos"), which appears to be a Moscow, Russia-based internet service provider. A sub-domain "m-13-9[.]canmos[.]ru," which is believed to be a sub-domain related

to M-13, is associated to the Second 89 IP Address.[32] A historical DNS query indicates that another one of M-13's sub-domains sip[.]m13[.]su also resolved to the Second 89 IP Address at various times in 2016, 2017, and 2018.

113. As noted above, M-13 provides, among other things, penetration testing services. Pen testing looks for exploitable vulnerabilities in computer systems that could be leveraged by attackers.

114. Based on my review of records obtained during the course of this investigation, I have learned that KLYUSHIN, ERMAKOV, and RUMIANTCEV used the Second 89 IP Address to access certain resources from the Tech Company between November 2018 and September 2020. RUMIANTCEV did so on November 28, 2018—approximately six days after the Second 89 IP Address was used to access a Namecheap account that is linked to the Neumann Account. As noted above, the Neumann Account was provided to 99Stack in connection with the lease of the Vultr infrastructure used to compromise FA 1, and the IP address used to register the Neumann Account (*i.e.*, the First 89 IP Address) was used to access earnings-related files associated with FA 2's publicly traded clients.

115. In 2020, KLYUSHIN, ERMAKOV, and RUMIANTCEV all used the Second 89 IP Address to send messages to each other and others. In KLYUSHIN's case, he accessed the private banking arm of Russian Standard Bank from the Second 89 IP Address on or about January 29, 2020.

---

[32] In general, a sub-domain is a separate part of the website that operates under the same primary domain name. Additionally, based on publicly available information, one of M-13's mail servers resolves to IP address 89.107.124.38.

Conclusion

116. For the foregoing reasons, there is probable cause to believe that KLYUSHIN, ERMAKOV, SLADKOV, IRZAK, and RUMIANTCEV conspired, in violation of Title 18, United States Code, Section 371, to commit computer intrusion, contrary to Title 18, United States Code, Section 1030(a)(4); wire fraud, contrary to Title 18, United States Code, Section 1343, and securities fraud, contrary to Title 15, United States Code, Sections 78j(b) and 78ff(a).

Respectfully submitted,

BJ Kang by MBB
BJ Kang
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to me telephonically on this 20 day of March, 2021

Marianne B. Bowler, USMJ
HONORABLE MARIANNE B. BOWLER
UNITED STATES MAGISTRATE JUDGE