

AAS:TAD/MEB/DKK  
F. #2018R00364

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

-----X

UNITED STATES OF AMERICA

- against -

VYTAUTAS PARFIONOVAS,



Defendant.

-----X

AMENDED AFFIDAVIT  
AND COMPLAINT IN  
SUPPORT OF AN  
APPLICATION FOR  
AN ARREST WARRANT

(T. 15, U.S.C., §§ 78j(b) and 78ff;  
T. 18, U.S.C., §§ 371, 1028A(a)(1),  
1028A(b), 1028A(c)(4), 1028A(c)(5),  
1029(a)(1), 1029(a)(2), 1029(a)(3),  
1029(a)(5), 1029(b)(b)(2), 1030(a)(4),  
1030(b), 1030(c)(3)(A), 1343, 1349,  
1956(h), 2 and 3551 et seq.)

No. 17-M-883

EASTERN DISTRICT OF NEW YORK, SS:

CARRIE CROT, being duly sworn, deposes and states that she is a Special Agent with the Federal Bureau of Investigation, duly appointed according to law and acting as such:

Count One: Computer Intrusions

In or about and between January 2011 and March 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as

together with others, did knowingly and with the intent to defraud access, and attempt to access, one or more protected computers without

authorization, and by means of such conduct further the intended fraud and obtain something of value, to wit: information, United States currency and the use of computers.

(Title 18, United States Code, Sections 1030(a)(4), 1030(b), 1030(c)(3)(A), 2 and 3551 et seq.)

Count Two: Conspiracy to Commit Computer Intrusions

In or about and between January 2011 and March 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as [REDACTED] [REDACTED] together with others, did knowingly and intentionally conspire and agree with others to commit offenses against the United States, to wit: to access one or more protected computers with the intent to defraud and without authorization, and by means of such conduct further the intended fraud to obtain anything of value, to wit: information, United States currency and the use of computers, contrary to Title 18, United States Code, Sections 1030(a)(4) and 1030(c)(3)(A).

(Title 18, United States Code, Sections 371 and 3551 et seq.)

Count Three: Conspiracy to Commit Money Laundering

In or about and between January 2011 and March 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as [REDACTED] [REDACTED] together with others, did knowingly and intentionally conspire: (a) to conduct one or more financial transactions affecting interstate and foreign commerce, to wit: interstate and foreign transfers of funds, which transactions in fact involved the proceeds of specified unlawful activity, to wit: aggravated identity theft, in

violation of Title 18, United States Code, Section 1028A, access device fraud, in violation of Title 18, United States Code, Section 1029, computer intrusions, in violation of Title 18, United States Code, section 1030, wire fraud, in violation of Title 18, United States Code, Section 1343, and fraud in the sale of securities, in violation of Title 15, United States Code, Sections 78j(b) and 78ff (collectively, the “Specified Unlawful Activities”), knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, with the intent to promote the carrying on of the Specified Unlawful Activities, contrary to Title 18, United States Code, Section 1956(a)(1)(A)(i); (b) to conduct one or more financial transactions affecting interstate and foreign commerce, to wit: interstate and foreign transfers of funds, which transactions in fact involved the proceeds of the Specified Unlawful Activities, knowing that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, and knowing that the financial transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership and control of the proceeds of the Specified Unlawful Activities, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i); and (c) to transport, transmit, or transfer a monetary instrument or funds from a place in the United States to or through a place outside the United States, with the intent to promote the carrying on of the Specified Unlawful Activities, contrary to Title 18, United States Code, Section 1956(a)(2)(A).

(Title 18, United States Code, Sections 1956(h) and 3551 et seq.)

Count Four: Wire Fraud

Upon information and belief, in or about and between January 2011 and March 2018, both dates being approximate and inclusive, within the Eastern District of New

York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as [REDACTED] together with others, did knowingly and intentionally devise a scheme and artifice to defraud: (a) individual accountholders at U.S. and foreign financial institutions, including securities brokerage firms (“Intrusion Victims”); and (b) U.S. and foreign financial institutions, including securities brokerage firms (“Targeted Financial Institutions”), and to obtain money and property from Intrusion Victims and Targeted Financial Institutions by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, transmitted and caused to be transmitted by means of wire communication in interstate and foreign commerce writings, signs, signals, pictures and sounds, including:

Date of Wire Communication	Type of Wire Communication
April 22, 2013	Email to Intrusion Victim’s financial advisor using Intrusion Victim’s AOL email account, instructing financial advisor to wire transfer \$225,000 from Intrusion Victim’s account to a bank account in the U.K.
May 7, 2013	Use of the Internet to open an online account at Financial Institution 3 in name of two Intrusion Victims and to transfer the Intrusion Victims’ cash and securities in an online account at Financial Institution 1 to Financial Institution 3
May 2, 2016	Use of an Internet Protocol (“IP”) address in Queens, New York, to hide PARFIONOVAS’s identity and location while accessing an Intrusion Victim’s online account at Data Company 1
July 6, 2017	Use of an IP address in Patchogue, New York, to hide PARFIONOVAS’s identity and location while accessing an Intrusion

	Victim's online account at Financial Institution 4 to attempt to place unauthorized stock trades from the Intrusion Victim's account
--	--

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

Count Five: Conspiracy to Commit Wire Fraud

Upon information and belief, in or about and between January 2011 and March 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as [REDACTED] together with others, did knowingly and intentionally conspire to defraud Intrusion Victims and Targeted Financial Institutions, and to obtain money and property from them by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, to transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce writings, signs, signals, pictures and sounds, contrary to Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

Count Six: Access Device Fraud


Upon information and belief, in or about and between January 2011 and March 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as [REDACTED] together with others, did knowingly and with intent to defraud: (1) traffic in and use in one or more unauthorized access devices during any one-year period, and by such conduct obtain anything of value

aggregating \$1,000 or more during that period; (2) possess fifteen or more unauthorized access devices; and (3) effect transactions with one or more access devices issued to another person or persons, to receive payment or any other thing of value during any one-year period the aggregate value of which is equal to or greater than \$1,000, all of which conduct affected interstate and foreign commerce.

(Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3), 1029(a)(5), 2 and 3551 et seq.)

Count Seven: Conspiracy to Commit Access Device Fraud

Upon information and belief, in or about and between January 2011 and March 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as

 together with others, did knowingly and with intent to defraud conspire to: (1) traffic in and use in one or more unauthorized access devices during any one-year period, and by such conduct obtain anything of value aggregating \$1,000 or more during that period; (2) possess fifteen or more unauthorized access devices; and (3) effect transactions with one or more access devices issued to another person or persons, to receive payment or any other thing of value during any one-year period the aggregate value of which is equal to or greater than \$1,000, all of which conduct affected interstate and foreign commerce, contrary to Title 18, United States Code, Sections 1029(a)(2), 1029(a)(3) and 1029(a)(5).

(Title 18, United States Code, Sections 1029(b)(2) and 3551 et seq.)

Count Eight: Securities Fraud

Upon information and belief, in or about and between January 2013 and March 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as [REDACTED] together with others, did knowingly and willfully use and employ one or more manipulative and deceptive devices and contrivances, contrary to Rule 10b-5 of the Rules and Regulations of the United States Securities and Exchange Commission, Title 17, Code of Federal Regulations, Section 240.10b-5, by: (1) employing one or more devices, schemes and artifices to defraud; (2) making one or more untrue statements of material fact and omitting to state the material facts necessary in order to make the statements made, in light of the circumstances in which they were made, not misleading; and (3) engaging in one or more acts, practices and courses of business which would and did operate as a fraud and deceit upon one or more investors and potential investors in targeted companies, each of which was an issuer of a class of securities that was publicly traded in the United States (“Targeted Companies”), in connection with the purchase and sale of investments in the Targeted Companies, directly and indirectly, by use of means and instrumentalities of interstate commerce and the mails.

(Title 15, United States Code, Sections 78j(b) and 78ff; Title 18, United States Code, Sections 2 and 3551 et seq.)

Count Nine: Conspiracy to Commit Securities Fraud

Upon information and belief, in or about and between January 2013 and March 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as

[REDACTED] together with others, did knowingly and willfully conspire to use and employ manipulative and deceptive devices and contrivances, contrary to Rule 10b-5 of the Rules and Regulations of the United States Securities and Exchange Commission, Title 17, Code of Federal Regulations, Section 240.10b-5, by: (1) employing devices, schemes and artifices to defraud; (2) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in light of the circumstances in which they were made, not misleading; and (3) engaging acts, practices and courses of business which would and did operate as a fraud and deceit upon investors and potential investors in the Targeted Companies, in connection with the purchase and sale of investments in the Targeted Companies, directly and indirectly, by use of means and instrumentalities of interstate commerce and the mails, contrary to Title 15, United States Code, Sections 78j(b) and 78ff.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

Count Ten: Aggravated Identity Theft

Upon information and belief, in or about and between January 2011 and March 2018, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendant VYTAUTAS PARFIONOVAS, also known as

[REDACTED] together with others, during and in relation to the crimes charged in Counts One through Two and Counts Four through Seven, did knowingly and intentionally transfer, possess and use, without lawful authority, one or more means of identification of one or more persons, to wit: names, social security numbers, dates of birth, employer and taxpayer identification numbers, addresses, bank account numbers, investment account numbers, brokerage account numbers, other account



information, routing numbers, and unique electronic identification numbers including usernames and passwords, knowing that these means of identification belonged to said persons.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(4), 1028A(c)(5), 2 and 3551 et seq.)

The source of your deponent's information and the grounds for her belief are as follows:<sup>1</sup>

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been a Special Agent with the FBI since 2012. I am currently assigned to an FBI squad that investigates cybercrime. During my tenure with the FBI, I have participated in investigations that have included, among other crimes, access device fraud, fraud and related activity in connection with computers, wire fraud, money laundering, securities fraud and attempts and conspiracies to commit the same. I am familiar with the facts and circumstances set forth below from my participation in the investigation, my review of documents obtained pursuant to the investigation, and from reports of other law enforcement officers involved in the investigation.

2. On or about October 6, 2017, I swore to an affidavit and complaint in support of an arrest warrant for VYTAUTAS PARFIONOVAS, also known as [REDACTED] ("PARFIONOVAS"), before the Honorable Lois Bloom in the Eastern District of New York. On that date, Judge Bloom

---

<sup>1</sup> Because the purpose of this Complaint is to set forth only those facts necessary to establish probable cause to arrest, I have not described all the relevant facts and circumstances of which I am aware.

issued a warrant for PARFIONOVAS's arrest. This amended affidavit and complaint contains the same information as the initial affidavit and complaint, as well as supplemental information and charges against PARFIONOVAS, which have been added for purposes of effectuating PARFIONOVAS's extradition to the United States on all relevant charges.

**Relevant Definitions**

3. A "server" is a computer program designed to process requests and deliver data to other (client) computers over a local network or the Internet. There are different types of computer servers, including (a) web servers, which host web pages and run applications in connected-to web browsers; (b) email servers, which facilitate sending and receiving email messages; and (c) identity servers, which support logins and security roles for authorized users. All servers run on computers.

4. An Internet Protocol ("IP") address is a numerical identifier assigned to each device (e.g., computer, router, mobile device) participating in a computer network that uses the Internet Protocol for communication. IP addresses are usually written and displayed in human-readable notations, e.g., 123.45.255.9. An IP address serves two principal functions: host or network interface identification and location addressing. Because every device that connects to the internet uses an IP address, IP address information can identify computers and other devices that accessed the internet.

5. "Spamming" means using electronic messaging systems such as email to send unsolicited messages to multiple recipients. Spamming is often used in conjunction with phishing.

6. "Phishing" refers to the attempt to obtain sensitive information, such as usernames and passwords to bank or brokerage accounts, by masquerading as a trustworthy

entity in an email or other electronic communication. Phishing is typically carried out by email “spoofing” or instant messaging, and it often directs users to enter details at a fake website that is designed to appear almost identical to the legitimate one. Email “spoofing” is the creation of email messages with a forged sender address. A phishing attack might begin with a spoofed email to an individual claiming to originate from the victim’s bank. That spoofed email would contain a link to a web address that would look like the login page for the same bank but would in fact be a web address controlled by the criminal actors and would harvest the victim’s login and password for the criminal actors. Phishing emails may also contain links that, if clicked, can download malware onto a victim’s computer.

7. “Malware” refers to malicious computer software programmed to, among other things, gain and maintain unauthorized access to computers and to identify, store and export information from hacked computers.

8. “PHP script” is primarily used as a server-side scripting language designed for web development and general-purpose computer programming. An unauthorized PHP script is an unauthorized program designed to run undetected within a hacked server.

9. A media access control (“MAC”) address is a unique identification number assigned to a network interface such as a wireless or ethernet card attached to a computer.

10. A virtual private network (“VPN”) allows a user to, among other things, conceal a true IP address. When a device such a smartphone or computer is connected to a VPN, the device receives a new IP address from the VPN provider. All

traffic from the VPN-connected computer routes through the VPN network, so the true IP address assigned by the user's internet service provider is hidden.

11. A "security" is, among other things, any note, stock, bond, debenture, evidence of indebtedness, investment contract or participation in any profit-sharing agreement.

12. A "buy order" is an order by a stock trader to purchase a security.

13. A "sell order" is an order by a stock trader to sell a security.

14. A "short sale order" is a particular type of stock sale order where the stock trader agrees to sell a security that the stock trader does not presently own. Because the stock trader does not own the particular security, the stock trader must borrow it. Typically, in order to borrow the particular security, the stock trader holds a cash "margin" account at a brokerage house and uses that account as collateral to borrow the security. In borrowing the security, the stock trader agrees to sell the borrowed stock at a specified price in the future.

15. "Covering a short" refers to buying back borrowed securities to close an open short position. Covering a short involves purchasing the exact same security that one initially sold short. If a stock trader is able to cover a short sale at a price less than the short sale price, the stock trader will make money—specifically, the difference between the short sale price and the cover price.

16. "Regular trading hours" and "regular trading days" refers to the time period from 9:30 a.m. to 4:00 p.m. EST from Monday through Friday, excluding applicable holidays, during which most stock trading on major stock exchanges in the United States

occurs. Major stock exchanges include the New York Stock Exchange (“NYSE”) and the Nasdaq Stock Market.

17. “Pre-market trading” refers to the period of trading activity that occurs before regular trading hours. The pre-market trading session typically spans from approximately 4:00 a.m. to 9:30 a.m. EST on regular trading days.

18. “After-hours trading” refers to the period of trading activity that occurs after regular trading hours. The after-hours trading session typically spans from 4:00 p.m. to 8:00 p.m. EST on regular trading days.

**The Defendant and CC-1**

19. PARFIONOVAS, also known as [REDACTED]

[REDACTED] is a [REDACTED] Lithuanian national who currently resides in [REDACTED] Ukraine.

20. Co-Conspirator 1 (“CC-1”) is a [REDACTED]  
[REDACTED]

**Overview of the Fraudulent Scheme**

21. Since approximately 2011, PARFIONOVAS, CC-1 and others engaged in a scheme to obtain unauthorized access to protected computers, specifically: U.S.-based email servers and computer servers that allow U.S. customers to access their bank accounts and securities brokerage accounts over the Internet. The email accounts, online bank accounts and online securities brokerage accounts belonged to victims in the Eastern District of New York and elsewhere (“Victim Accounts”).

22. To gain access to the Victim Accounts, PARFIONOVAS, CC-1 and others obtained customer login information (commonly referred to as “logins”), including

usernames and passwords. PARFIONOVAS, CC-1 and others obtained the customer login information through phishing and computer intrusions, commonly referred to as hacking.

23. After obtaining unauthorized access to the Victim Accounts, PARFIONOVAS, CC-1 and others used the Victim Accounts to commit money laundering, wire fraud, access device fraud, securities fraud and other crimes by means including the following:

- a. **Email accounts:** After obtaining login information for victim email accounts, PARFIONOVAS, CC-1 and others accessed the accounts without authorization and often read victims' emails to familiarize themselves with the victims' style of writing and contacts. Using the victims' email accounts, PARFIONOVAS, CC-1 and others sent messages to the victims' financial advisers requesting wire transfers from the victims' financial institutions to overseas bank accounts controlled by the co-conspirators.
- b. **Online securities brokerage accounts:** After obtaining login information for victim online securities brokerage accounts, PARFIONOVAS, CC-1 and others accessed the accounts without authorization and stole money from victims in a variety of ways. Sometimes, the co-conspirators used ACATS ("Automated Customer Account Transfer Service"), which facilitates the transfer of securities from one account to another at a different firm. To do this, PARFIONOVAS, CC-1 and others used the victim's login credentials to access the victim's existing securities brokerage

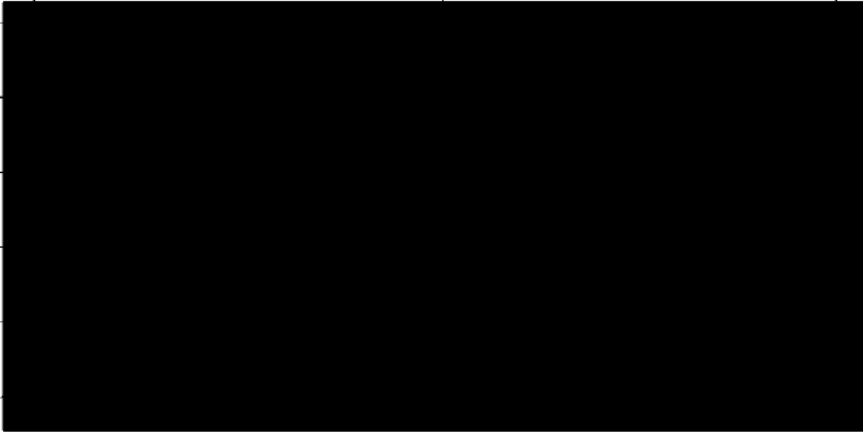
account. Using personal identifying information (“PII”) found therein, PARFIONOVAS and his co-conspirators opened a new account in the victim’s name at a different financial institution.

PARFIONOVAS, CC-1 and others then transferred the victim’s entire existing online securities account to the new account, which PARFIONOVAS and his co-conspirators controlled.

PARFIONOVAS, CC-1 and others sold existing securities positions in the new account and/or wire transferred the proceeds to overseas bank accounts they controlled. When financial institutions began to detect and block the ACATS scheme, PARFIONOVAS, CC-1 and others obtained unauthorized access to victim online brokerage accounts and conducted unauthorized trades in the victim accounts, for the benefit of accounts the co-conspirators controlled. The latter scheme is explained in more detail below at pages 26 to 37.

#### **Email and Social Media Accounts Controlled by PARFIONOVAS and CC-1**

24. To facilitate the fraudulent scheme, PARFIONOVAS and CC-1 used multiple email and social media accounts hosted by U.S. providers of electronic communications services, including Apple, Google, Yahoo and Facebook. To hide their identities, locations and their connection to criminal activity, PARFIONOVAS and CC-1 registered these email and social media accounts under false names and often used VPNs to access them. As explained in more detail below, records obtained pursuant to subpoenas and search warrants establish that PARFIONOVAS controlled the following email and social media accounts, among others:

Provider	Account	Timeframe Used
Google		
Yahoo		
Facebook		
Apple		
Google		

Records obtained pursuant to subpoenas and search warrants establish that CC-1 controlled the following email and social media accounts, the names of which have been disguised because CC-1 is at large and unaware of the FBI's investigation: (1) CC-1 Yahoo Account 1; (2) CC-1 Yahoo Account 2; and (3) CC-1 Facebook.

**Examples of Computer Intrusions, Wire Fraud, Money Laundering, Access Device Fraud and Aggravated Identity Theft in 2013**

**A. EDNY Victims G.G. and J.G.**

25. In April 2013, PARFIONOVAS, CC-1 and others conspired to obtain unauthorized access to a protected computer, specifically, an AOL email server, in furtherance of a scheme to fraudulently transfer \$225,000 from a trust account that belonged to victims who lived in the Eastern District of New York ("Victim G.G." and "Victim J.G.") to an overseas bank account controlled by PARFIONOVAS and CC-1. After obtaining unauthorized access to Victim G.G.'s AOL email account, PARFIONOVAS, CC-1 and others read Victim G.G.'s emails, including emails Victim G.G. had previously sent to Financial Institution 1, a U.S. Financial Institution known to the FBI. Pretending to be Victim G.G., PARFIONOVAS and CC-1 sent emails from Victim G.G.'s AOL account



requesting a \$225,000 wire transfer from a Financial Institution 1 trust account in Victim G.G. and Victim J.G.'s names to an overseas bank account controlled by CC-1 and PARFIONOVAS. Emails obtained pursuant to search warrants reveal extensive communications between PARFIONOVAS and CC-1 about the scheme. Documents obtained from Financial Institution 1 confirm that Victim G.G. did not send the email requesting the \$225,000 transfer and that Victim G.G. did not authorize anyone to request the transfer on his/her behalf.

26. Using Yahoo messenger, a chat function that allows users to communicate in real time, PARFIONOVAS sent messages from [REDACTED] (" [REDACTED] Yahoo") to CC-1 Yahoo Account 1 about how to transfer money out of Victim G.G. and Victim J.G.'s account at Financial Institution 1. On or about April 16, 2013, PARFIONOVAS, using [REDACTED] Yahoo, sent CC-1 the following information: a username, password, and IP address for Victim G.G. and Victim J.G., Victim G.G. and Victim J.G.'s dates of birth ("DOB"), Victim G.G.'s social security number ("SSN") and address in Port Washington, New York, and the value of securities in Victim G.G. and Victim J.G.'s account at Financial Institution 1. PARFIONOVAS instructed CC-1: "you need to transfer from [Financial Institution 1 account number] to [Financial Institution 1 account number]." CC-1 responded: "damn never called before what info they even ask lol,"<sup>2</sup> which I believe means that CC-1 had never before called Financial Institution 1 to request a wire transfer, and he did not know what identifying information Financial Institution 1 would require to verify the account. PARFIONOVAS responded: "just call." Using [REDACTED] Yahoo, PARFIONOVAS

---

<sup>2</sup> Spelling and grammatical errors in the emails and messages reprinted herein appeared in the original emails and have not been corrected, unless indicated in brackets.

again gave CC-1 Victim G.G.'s name, stating: "u are that guy," i.e., that CC-1 would pose as Victim G.G. when calling Financial Institution 1. CC-1 responded: "so wanna tr[ansfer] shit? From one acc to another? Am [Victim G.G]?" PARFIONOVAS responded affirmatively and instructed CC-1 to transfer \$50,000 from one of Victim G.G. and Victim J.G.'s accounts at Financial Institution 1 to a different account in the same victims' names at Financial Institution 1.

27. Later Yahoo chats between PARFIONOVAS and CC-1 indicate that CC-1 telephoned Financial Institution 1 to try to initiate the wire transfer, but a Financial Institution 1 representative asked CC-1 "who my financial adviser is that handle my account," so CC-1 pretended he had a bad telephone connection and hung up ("she ask who my financial advisor is . . . so I said hello hello like phone cut [] off"). On or about April 16, 2013, after the unsuccessful phone call, PARFIONOVAS and CC-1 discussed using Victim G.G.'s AOL email account to initiate the wire transfer instead of the phone.

28. On or about April 16, 2013, CC-1 sent a series of messages to PARFIONOVAS at [REDACTED] Yahoo, indicating PARFIONOVAS had access to Victim G.G.'s AOL email account, such as: "Check inside his email . . . he emailed him before? . . he email account advisor before? . . . cuz some talk with email they don't like calling check his email." PARFIONOVAS responded: "oh fuck many emails . . . sick shit . . . they wrote to [Financial Institution 1] . . . with all fucking info . . . so nice doc." PARFIONOVAS added: "he tell all shit on email . . . sell stocks . . . send money." PARFIONOVAS and CC-1 then decided that CC-1 would send an email from Victim G.G.'s AOL email account to Victim G.G.'s financial adviser instructing the financial adviser to do the wire transfer.

PARFIONOVAS added that they "need to change that phone," meaning that they needed to

change the phone number for Victim G.G. and Victim J.G.'s account so Financial Institution 1 did not call the real accountholder to verify the wire transfer. PARFIONOVAS and CC-1 discussed that once they sent the email to Victim G.G.'s financial adviser, they needed "to sit on that fucking email," i.e., monitor Victim G.G.'s AOL email account. Noting that Victim G.G.'s AOL email account was linked to his iPhone, and Victim G.G. would see incoming emails from his financial adviser on his iPhone, PARFIONOVAS stated: "need sit and fucking delete + i can do some things and he won't see."

29. On or about April 17, 2013—a Wednesday—PARFIONOVAS and CC-1 discussed waiting until the following Monday to send the email to Victim G.G.'s financial adviser. CC-1 Yahoo Account 1 wrote, "I told you . . . Just relax." PARFIONOVAS, using [REDACTED] Yahoo, responded: "yeah . . . monday maybe . . . need to prepare form nice."

30. On or about April 22, 2013—the following Monday—PARFIONOVAS, using [REDACTED] Yahoo, exchanged messages with CC-1 Yahoo Account 1 about what to write in the email to Victim G.G.'s financial adviser, whose first name was "Joel." PARFIONOVAS advised CC-1 to "write good morning Joel," and to state that Victim G.G. needed to wire "225" to a bank account in the U.K. On the same date, CC-1 Yahoo Account 2 sent an email to [REDACTED] ("[REDACTED] Gmail") that included the business name, "sort code,"<sup>3</sup> IBAN number,<sup>4</sup> bank name, business address and account

<sup>3</sup> A sort code is an identification number used by British and Irish banks.

<sup>4</sup> IBAN stands for international bank account number and consists of up to thirty-four alphanumeric characters consisting of a country code, two check digits, and a number that includes the domestic bank account number, branch identifier and potential routing information.

number ending in -7895 for a bank account held at a U.K. financial institution known to the FBI (the “-7895 Account”). The following language appeared in the text of the email after the -7895 Account information:

Good Morning Joel,

Attached please find a transfer instruction for \$225,000 to be transferred on my behalf to The Local Shopping REIT plc London for investment reasons as soon as possible, make sure it done this morning as I want the payment to get there ASAP. . Once the transfer is complete please respond to this email to notify me so i can inform my lawyer.

Thank You

[Victim G.G.]

31. On the same date, PARFIONOVAS, using [REDACTED] Gmail, responded to the above email by sending an email with the attachment

“transfer\_instructions\_for\_uk.bmp.” The attachment read, in relevant part:

“Please wire from my account, xxxx5557, the [name redacted] Revocable Trust the sum of \$225,000 to the below instructions”

Thank You,

[scanned signature of Victim G.G.]

Information for conducting a wire transfer to the -7895 Account appeared below Victim G.G.’s scanned signature.

32. On the same date, using [REDACTED] Gmail, PARFIONOVAS sent CC-1 Yahoo Account 2 an email containing Victim G.G. and Victim J.G.’s names, Victim G.G.’s DOB, SSN, AOL email address, phone numbers, home address in Port Washington, New York, and the number of an account ending in -5557, which was held in Victim G.G. and Victim J.G.’s name at Financial Institution 1 (the “-5557 Account”). The email also

included a detailed breakdown of the dollar value of stock positions in the -5557 Account and the name, email address, phone number and business address of Victim G.G.'s financial adviser at Financial Institution 1, whose first name was "Joel."

33. Documents obtained from Financial Institution 1 show that on April 22, 2013, a Financial Institution 1 investment adviser named "Joel" received an email from Victim G.G.'s AOL email account that contained a request to transfer \$225,000 from the -5557 Account to the -7895 Account. The email contained the subject line: "wire to transfer to U.K.," and was copied to a Financial Institution 1 employee with the first name "Sarah." The email from Victim G.G.'s AOL email account contained the same attachment with wiring instructions that PARFIONOVAS had sent from [REDACTED] Gmail to CC-1 Yahoo Account 2. Financial Institution 1 did not process the wire transfer because it determined "the client," i.e., Victim G.G., "did not send or sign this letter."

34. On April 22, 2103, PARFIONOVAS, using [REDACTED] Yahoo, exchanged messages with CC-1, stating that "she," i.e., Sarah, the Financial Institution 1 employee, "wrote some shit." PARFIONOVAS then appeared to quote an email from Sarah to Victim G.G., stating: "Greg, Here is a copy of the email sent to Joel and I. Thanks!" PARFIONOVAS added: "fuck me . . . I think they contacted him" and "it looks like he fucking talked on phone with her."

**B. Victims D.R. and K.W.**

35. On or about and between April 30, 2013 and May 20, 2013 PARFIONOVAS and CC-1 stole approximately \$50,000 from a Financial Institution 3 account held in the names of two individuals whose identities are known to the FBI ("Victim D.R." and "Victim K.W."), through a series of unauthorized transactions. First,

PARFIONOVAS and CC-1 transferred Victim D.R. and Victim K.W.'s entire existing securities account at Financial Institution 1 to Financial Institution 3, a U.S. financial institution known to the FBI, using ACATS. Documents obtained from Financial Institutions 1 and 3 reveal that Victims D.R. and K.W. did not initiate or authorize the transfer. Notably, the Financial Institution 3 account that received the total account transfer was opened using [REDACTED] Gmail, one of PARFIONOVAS's email accounts. Once the Victim Account had been transferred to Financial Institution 3, CC-1 and others called Financial Institution 3, pretending to be an owner of the account, and requested a \$50,000 wire transfer to the -7895 Account, discussed above. Documents from Financial Institution 3 and emails between PARFIONOVAS and CC-1 show that Financial Institution 3 transferred \$50,000 to the -7895 Account.

36. On or about April 30, 2013, PARFIONOVAS sent messages from [REDACTED] Yahoo to CC-1 Yahoo Account 1 about getting "alot" of Financial Institution 1 accounts "to spam." PARFIONOVAS stated that by the following day, he should have "like 100 login." On or about May 7, 2013, PARFIONOVAS sent messages from [REDACTED] Yahoo to CC-1 Yahoo Account 1 about obtaining online access to customer accounts at Financial Institution 1. PARFIONOVAS stated, in relevant part: "fucking [Financial Institution 1] . . .so nice . . . now will transfer few to [Financial Institution 2] . . . now I see how they work bastards . . . sometimes I can't login . . . but after cookies die I can . . . so we wait . . . and I can login after." PARFIONOVAS added: "then we fuck same name." CC-1 responded: "wire." PARFIONOVAS responded: "as u see they didn't want send." CC-1 responded: "but they will if same name bro . . . less doubt." Based on my training, experience and knowledge of the investigation, including documents and information received from Financial Institution 1,

I believe the above-quoted chats refer to obtaining unauthorized access to Victim Accounts at Financial Institution 1 and transferring them to other brokerage firms. I believe the phrase “then we f--- same name” means opening a new account at a different brokerage firm in the same victim’s name to receive the transfer.

37. On or about May 7, 2013, PARFIONOVAS, together with CC-1 and others, opened an online account ending in -6906 (the “-6906 Account”) at Financial Institution 3 in the names of Victim D.R. and Victim K.W. Online account opening documents obtained from Financial Institution 3 for the -6906 Account included Victim D.R. and Victim K.W.’s full names, DOBs, SSNs, mothers’ maiden names, and addresses. [REDACTED] Gmail appeared as the email address for the -6906 Account. The phone number for the -6906 Account was (516) 858-4443, a telephone number sent to [REDACTED] Gmail by Spoofcard, a company that allows users to change or “spoof” the caller ID number of the phone number from which they are calling. On or about May 7, 2013, [REDACTED] Gmail received an automated email from Financial Institution 3 referencing the -6906 Account and thanking Victim D.W. for opening an account at Financial Institution 3. On the same date, Financial Institution 1 received a request for an ACATS transfer of Victim D.R. and Victim K.W.’s existing account, ending in -1546 (the “1546 Account”) to the -6906 Account. Financial Institution 1 eventually processed the ACATS transfer, and the -6906 Account received approximately \$260,000 in cash and securities from the -1546 Account.

38. On or about May 8, 2013, PARFIONOVAS sent messages from [REDACTED] Yahoo to CC-1 Yahoo Account 1, telling CC-1 to call Financial Institutions 1 and 3 to check on the status of the transfer from the -1546 Account to the -6906 Account. In the messages,

PARFIONOVAS sent CC-1 Victim D.R. and Victim K.W.'s names, DOBs, SSNs, mothers' maiden names, and address to facilitate answering security questions.

39. On or about May 15, 2013, PARFIONOVAS sent messages from [REDACTED] Yahoo to Co-Conspirator 2 ("CC-2"), an individual whose identity is known to the FBI, instructing CC-2 to "go to Skype," and telling CC-2 "we doing wire to UK from [Financial Institution 3]," "I tra[ns]fered account" and "money there." PARFIONOVAS then sent CC-2 details of the -6906 Account, including the account value, cash balance and stock buying power. On the same date, PARFIONOVAS instructed CC-2 to call Financial Institution 3 to initiate a wire transfer "to UK." PARFIONOVAS sent CC-2 Victim D.R. and Victim K.W.'s names, SSNs, DOBs and address.

40. On or about May 15, 2013, PARFIONOVAS used [REDACTED] Yahoo to communicate with CC-1 and CC-2 about the UK account (the -7895 Account) that would receive the \$50,000 wire transfer from the -6906 Account. During a chat session with CC-2, PARFIONOVAS sent CC-2 a web link to the fax he had sent to Financial Institution 3 requesting the wire transfer. CC-2 responded, in relevant part, that PARFIONOVAS had put the wrong IBAN number for the -7895 Account on the fax. PARFIONOVAS later responded that he had "fixed iban."

41. On or about May 16, 2013, using [REDACTED] Yahoo, PARFIONOVAS sent messages to CC-1 Yahoo Account 1 instructing CC-1 to call Financial Institution 3 to find out "if wire done." On the same date, [REDACTED] Gmail received an email from Financial Institution 3 to Victims D.R. and K.W. stating, in relevant part: "we've received you're wire request in the amount of \$50,000.00."



42. Information obtained by Financial Institution 3 shows that, on or about May 15, 2013, multiple stock positions were liquidated in the -6906 Account. Moreover, on or about May 16, 2013, a \$50,000 international wire was sent to the -7895 Account, the same U.K. bank account discussed in paragraphs 29 to 34, above.

43. On or about May 17, 2013, CC-1 sent messages to [REDACTED] Yahoo stating that the “50 came,” i.e., the \$50,000 had arrived in the -7895 Account. PARFIONOVAS responded: “send my 25 cash my share I will give account.” On or about May 20, 2017, PARFIONOVAS sent CC-1 the name of an individual in Kharkov, Ukraine, to whom CC-1 should send the money via Western Union and MoneyGram.

**Examples of Computer Intrusions, Money Laundering, Wire Fraud, Access Device Fraud and Securities Fraud in 2015 and 2016**

44. In or about and between January 2013 and March 2018, both dates being approximate and inclusive, PARFIONOVAS, CC-1 and others conspired to and did access without authorization computer servers that hosted online securities brokerage accounts of Intrusion Victims who resided in the Eastern District of New York and elsewhere (“Victim Brokerage Accounts”), and committed securities fraud in securities of Targeted Companies, each of which was an issuer of a class of securities that was publicly traded in the United States, that benefitted accounts belonging to members of the conspiracy. After obtaining unauthorized access to the Victim Brokerage Accounts, PARFIONOVAS stole money from the Victim Brokerage Accounts in a variety of ways. Specifically, PARFIONOVAS and his co-conspirators fraudulently used the Victim Brokerage Accounts to place unauthorized trades that benefitted accounts that belonged to PARFIONOVAS and his co-conspirators (“Aggressor Accounts”). To fund the unauthorized trades, PARFIONOVAS and his co-

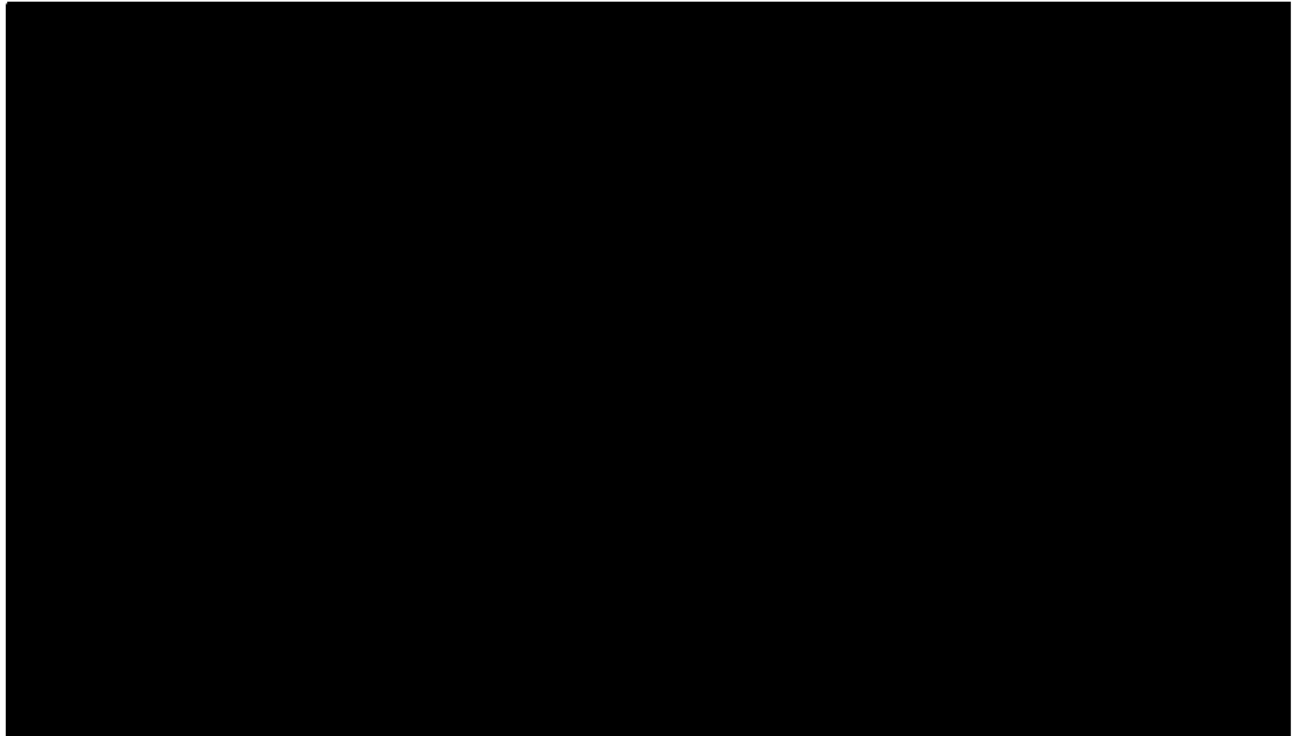
conspirators sometimes fraudulently liquidated existing stock positions held by the Victim Brokerage Accounts, among other things.

45. PARFIONOVAS and his co-conspirators used the Aggressor Accounts to place short sale orders for securities in the Targeted Companies at prices above the prevailing market prices during pre-market and after-hours trading. At or about the same time, PARFIONOVAS and his co-conspirators fraudulently used the Victim Brokerage Accounts to place buy orders at prices that matched the short sale orders placed by PARFIONOVAS and his co-conspirators. In so doing, PARFIONOVAS and his co-conspirators executed their short sale orders at artificially high prices.

46. After the short sale transactions were completed, PARFIONOVAS and his co-conspirators covered their short sales in two principal ways. First, PARFIONOVAS and his co-conspirators used the Aggressor Accounts to purchase securities of the Targeted Companies at the prevailing market prices, which were below the short sale prices and therefore allowed PARFIONOVAS and his co-conspirators to profit. Second, PARFIONOVAS and his co-conspirators fraudulently used the Victim Brokerage Accounts to sell securities of the Targeted Companies to PARFIONOVAS and his co-conspirators at prices below the prevailing market prices and therefore allowed PARFIONOVAS and his co-conspirators to profit.

47. PARFIONOVAS and his co-conspirators also used the Victim Brokerage Accounts to favorably manipulate the prices of securities of the Targeted Companies held by PARFIONOVAS and his co-conspirators in the Aggressor Accounts. For example, PARFIONOVAS fraudulently used the Victim Accounts to make a series of purchases of a security that PARFIONOVAS and his co-conspirators held to artificially increase the price of

the security, and PARFIONOVAS and his co-conspirators then sold the security to earn a profit.



**B. The Conspiracy Brokerage Firm A Account**

49. In or about January 2016, PARFIONOVAS, using [REDACTED] Yahoo, exchanged messages with CC-1 about opening an online brokerage account at a U.S. brokerage firm known to the FBI (“Brokerage Firm A”). They discussed funding the brokerage account from CC-1 BoA.

50. On or about February 14, 2016, PARFIONOVAS and CC-1 agreed that CC-1 would open an account at Brokerage Firm A under CC-1’s name, but using a passport with a “fake dob and face . . . and place of birth.”

51. On or about February 22, 2016, using [REDACTED] Yahoo, PARFIONOVAS explained to CC-1 how the scheme worked, stating: “I take some fraud logins. Do some shit

with stock . . . sometimes 2-3 in day . . . manipulation is 100% . . . there is some stocks u can do eas[ly] . . . some drug stocks.”

52. On or about February 26, 2016, PARFIONOVAS and CC-1 opened an online brokerage account in CC-1’s name at Brokerage Firm A (the “Conspiracy Brokerage Firm A Account”). To open Conspiracy Brokerage Firm A Account, CC-1 was required to submit a scanned image of his passport and a document containing his address. The passport and utility bill used to open Conspiracy Brokerage Firm A Account were forged; the passport contained an image of a male who is not CC-1 and a date of birth different from CC-1’s. Furthermore, PARFIONOVAS, using [REDACTED] Yahoo, previously informed CC-1 that PARFIONOVAS was “waiting w[h]ile kid making fake passport + utility bill.” On or about March 3, 2016, CC-1 and PARFIONOVAS funded the Conspiracy Brokerage Firm A Account by transferring \$32,000 from CC-1 BoA.

### **C. PARFIONOVAS Hires CC-3 to Hack into Online Brokerage Firm Servers**

53. On or about February 18, 2016 CC-1 Yahoo Account 1 sent PARFIONOVAS, on [REDACTED] Yahoo, the Yahoo username of Co-Conspirator 3, an individual whose identity is known to the FBI (“CC-3”), who was “good at programming” and “can spam,” whom PARFIONOVAS should contact. On the same date, PARFIONOVAS, using [REDACTED] Yahoo, contacted CC-3. During this chat session, PARFIONOVAS referenced CC-1 and asked CC-3 if he wanted to “make some \$.” PARFIONOVAS asked CC-3 “what u worked before?” CC-3 responded, in relevant part: “spam,” “programming” and “hack.” CC-3 explained: “I hack to get tools then I spam.” After learning more about CC-3’s hacking skills, PARFIONOVAS agreed to pay CC-3 to hack into various protected computers, including computer servers that hosted Victim Brokerage Accounts.

54. On or about April 14, 2016, PARFIONOVAS, using [REDACTED] Yahoo, sent messages to CC-3 asking CC-3 to see if he could hack into the server of an order management company known to the FBI, which permits users to trade stocks online through their accounts at certain U.S.-based and foreign brokerage firms ("Data Company 1"). On the same date, PARFIONOVAS, using [REDACTED] Yahoo, told CC-3 "that's why I need u guys to setup nice shit . . . I am good in stocks market and etc. but need right tools." On or about April 15, 2016, PARFIONOVAS sent CC-3 the URL to a foreign brokerage firm known to the FBI ("Brokerage Firm B"), whose customers can use Data Company 1 to trade stocks.

55. On or about April 15, 2016, using [REDACTED] Yahoo, PARFIONOVAS sent CC-3 the URL to the login page of a U.S. brokerage firm known to the FBI ("Brokerage Firm C"), whose customers can use Data Company 1 to trade stocks. After receiving the URL, CC-3 wrote "php," which, based on my training, experience and knowledge of the investigation, means that Brokerage Firm C's website was written in php computer language. On the same date, CC-3 wrote to PARFIONOVAS on [REDACTED] Yahoo stating: "vuln[erability] like html spoof we can make fake page and send to victim . . . with the same link." Immediately thereafter, CC-3 sent PARFIONOVAS the URL for Data Company 1. On the same date, PARFIONOVAS wrote to CC-3: "if we can upload files to [their] server it helps?" CC-3 responded: "yep." PARFIONOVAS explained that Data Company 1 was the "main[] company who provide platform and trading website to all brands," including Brokerage Firms B and C. PARFIONOVAS and CC-3 then discussed whether it was easier to upload a file containing malicious code on Brokerage Firm B or C's website. PARFIONOVAS then sent CC-3 a series of messages indicating that PARFIONOVAS had uploaded a file to Brokerage Firm C's website under the guise of opening an account there.

Using computer software that permits users to remotely access a computer, PARFIONOVAS sent CC-3 a series of numbers to enter so CC-3 could see PARFIONOVAS's computer screen. PARFIONOVAS then asked CC-3 if he could see "where it uploading." CC-3 responded: "you have to guess." Later that same day, CC-3 stated he had "shells," i.e., malicious pieces of code that can be uploaded to a site to gain access to files stored on that site.

56. On or about April 15, 2016, CC-3 sent a message to PARFIONOVAS on [REDACTED] Yahoo stating: "bro, I got [Brokerage Firm C]" and "tell me what u need from that site." PARFIONOVAS responded: "user logins." CC-3 indicated he was "searching in its database" and he had "admins password." Based on my training, experience and knowledge of the investigation, an "admin password" is the password used by the administrator of a database or server. The administrator of a database generally has the ability to access all files on a database or server.

57. On or about April 16, 2016, PARFIONOVAS, using [REDACTED] Yahoo, sent messages to CC-1 Yahoo Account 1 stating: "you know what we got [Brokerage Firm C] admin . . . wanted to trade but now thinking maybe better to cash w[h]ile I have all access and info." PARFIONOVAS and CC-1 discussed whether they could wire money from Brokerage Firm C accounts to overseas accounts they controlled. PARFIONOVAS stated he could also "put fake positions with good price or something." CC-1 later advised: "better to go trade up and down and [] not direct fraud wire."

**D. PARFIONOVAS Trades Stocks Against Victim Brokerage Accounts****Intrusion Victim 1**

58. On or about and between April 18 and 19, 2016, multiple customer accounts at Brokerage Firm C were subjected to unauthorized access and unauthorized trading. For example, on or about April 18, 2016, a Brokerage Firm C account that belonged to a victim whose identity is known to the FBI (“Intrusion Victim 1”) was used to buy and sell over 100,000 shares of Cnova NV (“CNV”), one of the Targeted Companies, at prices ranging from \$2.91 to \$3.78 per share. On the same date, Brokerage Firm C sent an automated email to Intrusion Victim 1 stating: “you have exceeded your overnight buying power by \$244,000. This condition must be addressed immediately.” Shortly thereafter, Intrusion Victim 1 emailed Brokerage Firm C stating: “I didn’t make any purchase today and I was not able to log into my account . . . I suspect my account has been hacked.” At approximately the same time that Intrusion Victim 1’s account was used to buy and sell thousands of shares of CNV, the Conspiracy Brokerage Firm A Account bought and sold thousands of shares of CNV. As a result of the unauthorized trading in Intrusion Victim 1’s account, Brokerage Firm C lost approximately \$50,000.

59. On or about April 18, 2016, PARFIONOVAS, using [REDACTED] Yahoo, sent messages to CC-1 Yahoo Account 1 stating that he had lost money trading stocks that day. CC-1 told PARFIONOVAS to “stick to plan always and all good,” adding “if you not manipulate close that laptop . . . stop losing it after making it.”

60. On or about April 22, 2016, CC-1 asked PARFIONOVAS how much money they had made from online trading. PARFIONOVAS responded: “like 100k,” adding that he had “changed some things” and “won[']t loose . . . changed platform and etc.”

61. On or about April 26, 2016, CC-1 Yahoo Account 1 sent messages to PARFIONOVAS or ██████ Yahoo asking PARFIONOVAS how much money he had wired from the Conspiracy Brokerage Firm A Account to CC-1 BoA. CC-1 noted that BoA had “charg[ed]” \$1,200 in fees in one month. Records for CC-1 BoA show multiple purchases and withdrawals in Kharkov, Ukraine, where PARFIONOVAS lived, from March 2016 through April 2016. The same records show approximately \$1,213.73 in “service fees” for the statement ending on April 12, 2016.

62. On or about April 27, 2016, using ██████ Yahoo, PARFIONOVAS told CC-1 not to worry about the \$1,200 because “from now on we taking profit from broker.” PARFIONOVAS added: “yesterday I did 10K [in] 5 min,” but PARFIONOVAS needed “more accounts.”

63. On or about May 12, 2016, using ██████ Yahoo, PARFIONOVAS asked CC-1 if Brokerage Firm A had called him because they “wrote that they wana know about some trades.” CC-1 said no and asked “what’s wrong.” PARFIONOVAS responded: “I did f---- a lot today . . . 30k.” PARFIONOVAS then sent CC-1 an email he had received from Brokerage Firm A about trades involving the stock ticker EARS. PARFIONOVAS stated he would “trade some shit to loose some,” to avoid suspicion. PARFIONOVAS explained: “I worked premarket . . . less volume . . . so they see more.”

### **Intrusion Victim 2**

64. On or about May 12, 2016, during pre-market trading, the Conspiracy Brokerage Firm A Account placed short sale orders for 41,074 shares of EARS (Auris Medical Holdings AG), one of the Targeted Companies, at \$3.99 per share, which were executed against a Victim Brokerage Account at Brokerage Firm B that belonged to a



resident of the Eastern District of New York (“Intrusion Victim 2”). Notably, the closing price of EARS on May 11, 2016, was \$3.53, approximately 12% lower than \$3.99. At approximately the same time, Intrusion Victim 2’s account purchased 49,000 shares of EARS at prices ranging from \$3.99 to \$3.89 per share. The Conspiracy Brokerage Firm A Account then purchased to cover 41,074 shares of EARS from Intrusion Victim 2 and on the open market at prices ranging from \$3.20 per share to \$3.50 per share. This series of transactions generated a gross profit of approximately \$23,467 for the Conspiracy Brokerage Firm A Account. Intrusion Victim 2’s account lost approximately \$31,493.

65. In addition to using the Conspiracy Brokerage Firm A Account on May 12, 2016, to execute artificially high short sale orders and purchase to cover orders of EARS against Intrusion Victim 2’s account, PARFIONOVAS, together with Co-Conspirator 4 (“CC-4”), an individual whose identity is known to the FBI,<sup>5</sup> also used CC-4’s brokerage account at a U.S. based brokerage firm known to the FBI (“Brokerage Firm D”), to do the same thing, at approximately the same time, generating a gross profit of approximately \$6,210 in CC-4’s account at Brokerage Firm D. Twitter communications between PARFIONOVAS and CC-4 reveal that over one year prior to the EARS trades, PARFIONOVAS and CC-4 agreed to execute trades against Victim Brokerage Accounts and that CC-4 would send PARFIONOVAS’s share of the profits to PARFIONOVAS in bitcoin, a crypto-currency. From approximately April 2014 to August 2016, CC-4 sent bitcoin payments totaling approximately \$237,120 to bitcoin addresses provided by

---

<sup>5</sup> On November 8, 2017, a grand jury in the Eastern District of New York returned a four-count indictment charging CC-4 with wire fraud conspiracy, conspiracy to commit computer intrusions and securities fraud, securities fraud, and conspiracy to commit money laundering. See Docket No. 17-620 (MKB).

PARFIONOVAS. Using [REDACTED] Yahoo, PARFIONOVAS repeatedly discussed CC-4's role in the scheme with CC-1.

66. I interviewed Intrusion Victim 2, who stated, in sum and substance, that he/she had not executed any trades in EARS on May 12, 2016 and that he/she had not authorized anyone else to do so on his/her behalf. Intrusion Victim 2 stated, in sum and substance, that on May 12, 2016, he/she had twice attempted to log into his/her online trading account, and on each occasion, his/her account was "locked." Intrusion Victim 2 stated that he/she then called his/her broker and learned about the unauthorized trades.

67. Intrusion Victim 2's account at Brokerage Firm B placed trades using Data Company 1. As such, the unauthorized EARS trades described above were initiated by accessing Data Company 1's server. Data Company 1's records show that shortly before the above-described trades, Intrusion Victim 2's account was accessed from an IP address that was different from the IP addresses that normally accessed the account. In addition, on or about May 2, 2016, ten days before the unauthorized trading discussed above, Intrusion Victim 2's account at Data Company 1 was accessed from a device with a MAC address that had not accessed Intrusion Victim 2's account before, according to records provided by Data Company 1, and from an IP address in Queens, New York. On or about the same date, the password to Intrusion Victim 2's online trading account was changed.

68. Notably, the MAC address of the device that accessed Intrusion Victim 2's account at Data Company 1 on May 2, 2016, is the same MAC address that repeatedly accessed a Data Company 1 account that the Conspiracy Brokerage Firm A Account used to trade stocks. Records obtained from Apple show that this MAC address (beginning with F45C) was associated with a serial number for a 13.3 inch MacBook Pro registered to

██████████ at a post office address in Luxemburg, with no corresponding street address and an invalid zip code (the ██████████ MacBook”). The Apple ID ██████████ (“██████████ iCloud”) registered the ██████████ MacBook. The FBI obtained a search warrant for ██████████ iCloud. The return contained, among other things, multiple photographs of PARFIONOVAS, a photograph of a Lithuanian driver’s license in PARFIONOVAS’s name, and an October 2, 2016 train ticket from Kyiv, Ukraine, to Kharkov, Ukraine, in PARFIONOVAS’s name.

**E. PARFIONOVAS and CC-1 Wire Profits From the Conspiracy Brokerage Firm A Account to CC-1 BoA Account**

69. On or about and between March 11, 2016 and May 13, 2016, PARFIONOVAS and CC -1 transferred approximately \$104,000 from the Conspiracy Brokerage Firm A Account to CC-1 BoA. From March 2016 to June 2016, PARFIONOVAS used CC-1 BoA to make cash withdrawals and debit card purchases totaling approximately \$120,858.61. The majority of the cash withdrawals and purchases during this time occurred in Kharkov, Ukraine, where PARFIONOVAS lives. Prior Yahoo chats between CC-1 and PARFIONOVAS indicate that CC-1 gave PARFIONOVAS the debit card to CC-1 BoA to use in Ukraine.

**F. Communications Between PARFIONOVAS and CC-1 After the Conspiracy Brokerage Firm A Account is Frozen**

70. On or about May 25, 2016, the executing broker for Brokerage Firm A froze the Conspiracy Brokerage Firm A Account, which contained approximately \$100,000. On the same date, CC-1 sent PARFIONOVAS messages on ██████████ Yahoo, stating: “they blocked . . . we can’t even trade. Fuck me.” PARFIONOVAS responded: “it[]s because

[Data Company 1] platform . . . we hacked all that system . . . and I using [Data Company 1].”

72. On or about June 23, 2016, PARFIONOVAS, using [REDACTED] Yahoo, sent messages to CC-1 Yahoo Account 1 stating, in relevant part: “we fucked,” “they gave to court,” “th[ey] emailed,” and “all fucking case they sent.” Based on my knowledge of the investigation, “they emailed” refers to an email the SEC sent to a Tutanota email account (“the Tutanota Email Account”) containing a copy of the civil complaint against CC-1. Documents obtained from Brokerage Firm A show that the Tutanota Email Account was used to register the Conspiracy Brokerage Firm A Account. On or about June 24, 2016, CC-1 responded: “thank God not my real dob.” As discussed above, the passport used to open the Conspiracy Brokerage Firm A Account did not contain CC-1’s true date of birth or “dob.” On or about the same date, PARFIONOVAS advised CC-1: “most[] important to take out yahoo now . . . and reset phone.” CC-1 responded: “Jesus you fucked me . . . it[’]s not about what I did . . . you hacked shit.” CC-1 asked PARFIONOVAS if “they,” i.e., the SEC, had emailed about the “fake id.” PARFIONOVAS said “no.” PARFIONOVAS advised CC-1 to “tell that [you] invested to someone and di[d]n’t make any trade.” CC-1 asked: “they believe that id . . . that guy we made?” PARFIONOVAS responded: “yea . . . no link to [you].” CC-1 stated: “thank God fake id.” PARFIONOVAS instructed CC-1 to

“get f--- away from that phone and yahoo.” On or about the same date, PARFIONOVAS directed CC-1 to create an instant messaging account on a different platform than Yahoo.

**G. Additional Aggressor Accounts Used by PARFIONOVAS**

73. PARFIONOVAS, CC-1 and others continued to obtain unauthorized access to Victim Brokerage Accounts to conduct unauthorized stock trades that benefitted Aggressor Accounts that PARFIONOVAS and his co-conspirators controlled. Between 2014 and 2017, PARFIONOVAS and his co-conspirators used at least six additional Aggressor Accounts as part of the scheme. According to information and documents from some of the affected financial institutions, including brokerage firms, they lost over \$4,000,000 as a result of the scheme described herein.

**PARFIONOVAS is** [REDACTED]

74. There is probable cause to believe that the defendant VYTAUTAS PARFIONOVAS used the following electronic communications and social media accounts to engage in the criminal schemes described above: [REDACTED] Yahoo, [REDACTED] Gmail, a Facebook account with the username [REDACTED] (“[REDACTED] Facebook”), [REDACTED] iCloud, and the Gmail account [REDACTED] (“[REDACTED] Gmail”).

75. Czar Yahoo was created on or about February 18, 2013, from the IP address [REDACTED]. The text message recovery number for [REDACTED] Yahoo is [REDACTED]. [REDACTED] Czar Gmail was created on or about February 16, 2013, from the same IP address, with the same recovery number as [REDACTED] Yahoo. The recovery email address for both [REDACTED] Yahoo and [REDACTED] Gmail is [REDACTED]. As discussed in paragraphs 25 to 31 above, [REDACTED] Yahoo and [REDACTED] Gmail repeatedly sent communications to CC-1 Yahoo Accounts 1 and 2 about the same topics around the same time, including, for example, Victim G.G.’s

personally identifiable information. There is therefore probable cause to believe that the same person used and controlled [REDACTED] Yahoo and [REDACTED] Gmail.

76. On or about March 4, 2013, CC-1 Facebook sent Facebook direct messages to [REDACTED] Facebook stating: "I wrote you just now on email end [REDACTED]" adding: "wrote you all weekend tonnes email you even show like offline to me . . . yeah [REDACTED]." As discussed above, the complete email address for [REDACTED] Yahoo is [REDACTED]@yahoo.com. On the same date, [REDACTED] Facebook responded: "i am online . . . it showing u online . . ." CC-1 responded, via Facebook: "try message me . . . maybe delete[] and add agai[n]." On the same date, CC-1 Yahoo Account 1 sent messages to [REDACTED] Yahoo stating: "2 days and you not here . . . hello . . . hello . . ." Approximately twenty seconds after CC-1 sent the Facebook direct messages to [REDACTED] Facebook instructing him to try to send a message to CC-1 by deleting CC-1 as a contact and adding CC-1 again, [REDACTED] Yahoo sent the following Yahoo messages to CC-1 Yahoo Account 1: "wtf . . . now I got . . . 10000 messages . . . fucking computer." CC-1 Yahoo Account 1 responded: "TOLD YOU." Based on the overlapping timing and substance of these messages, there is probable cause to believe that the same person used and controlled [REDACTED] Yahoo and [REDACTED] Facebook.

77. Facebook records show that [REDACTED] Facebook was registered on or about December 6, 2009, in the name of [REDACTED] date of birth January 18, 1987. The email addresses for [REDACTED] Facebook are [REDACTED] Gmail and [REDACTED]@hotmail.com. According to Google records, VYTAUTAS PARFIONOVAS is the subscriber for [REDACTED] Gmail. Customs and Border Protection ("CBP") records reveal that in 2008, VYTAUTAS PARFIONOVAS submitted an ESTA (Electronic System for Travel Authorization)

application to travel to the United States. The ESTA application for PARFIONOVAS contained a date of birth of January 18, 1987 and the email address [REDACTED]@hotmail.com. Multiple images and videos contained in [REDACTED] Facebook depict the defendant VYTAUTAS PARFIONOVAS.<sup>6</sup> [REDACTED] Facebook repeatedly was accessed from the IP address [REDACTED] in 2014 and 2015, including on or about October 29, 2014. [REDACTED] Gmail repeatedly was accessed from the same IP address in 2014, including on or about October 27, 2014. In addition, [REDACTED] Yahoo repeatedly referred to locations, events and individuals specific to PARFIONOVAS.<sup>7</sup> There is therefore probable cause to believe that the defendant VYTAUTAS PARFIONOVAS used and controlled [REDACTED] Facebook, [REDACTED] Yahoo, [REDACTED] Gmail and [REDACTED] Gmail.

78. As discussed above, the MAC address of the device that accessed Intrusion Victim 2's account at Data Company 1 and the Conspiracy Brokerage Firm A Account is associated with the serial number of a computer registered by [REDACTED] iCloud.

[REDACTED]

[REDACTED]

The [REDACTED] iCloud search warrant return contained multiple images of PARFIONOVAS, including an image of a Lithuanian driver's license containing PARFIONOVAS's name, photograph and date of birth. [REDACTED] iCloud also contained screenshots of emails received by [REDACTED] Gmail and images posted by [REDACTED] Facebook. There is therefore probable cause to believe that the defendant VYTAUTAS PARFIONOVAS used and controlled [REDACTED] iCloud.

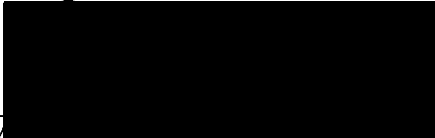
WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant VYTAUTAS PARFIONOVAS, also known as [REDACTED] [REDACTED] so that he may be dealt with according to law.

IT IS FURTHER REQUESTED that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including this Affidavit and the arrest warrant for the defendant VYTAUTAS PARFIONOVAS, with the exception that the complaint and arrest warrant can be unsealed for the limited purpose of disclosing the existence of, or disseminating, the complaint and/or arrest warrant to relevant United States, foreign, or intergovernmental authorities, at the discretion of the United States and in connection with efforts to prosecute the defendant or to secure the defendant's arrest, extradition or expulsion. Based on my training and experience, I have learned that criminals actively search for criminal affidavits on the Internet and disseminate them to other criminals as they deem appropriate, such as by posting them publicly through online forums.

Premature disclosure of the contents of this Affidavit and related documents will seriously



jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, and notify confederates.

  
CARRIE CROFT  
Special Agent  
Federal Bureau of Investigation

Sworn to before me this

9/11  
  
THE HONORABLE M  
UNITED STATES MA  
EASTERN DISTRICT