UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon.
	:	
v.	:	Crim. No. 15-
	:	
IVAN TURCHYNOV,	:	18 U.S.C. § 1349;
a/k/a "Ivan Turchinov,"	:	18 U.S.C. § 1343;
a/k/a "Ivan Turchinoff,"	:	15 U.S.C. §§ 78j(b) & 78ff, and
a/k/a "Vladimir Gopienko,"	:	17 C.F.R. § 240.10b-5;
a/k/a "DSU,"	:	18 U.S.C. § 371;
OLEKSANDR IEREMENKO,	:	18 U.S.C. § 1030;
a/k/a "Aleksandr Eremenko,"	:	18 U.S.C. § 1028A(a)(1);
a/k/a "Zlom,"	:	18 U.S.C. § 1956(h); and
a/k/a "Lamarez,"	:	18 U.S.C. § 2
ARKADIY DUBOVOY,	:	
IGOR DUBOVOY, and	:	
PAVEL DUBOVOY	:	

INDICTMENT

The Grand Jury in and for the District of New Jersey, sitting at Newark, charges:

At all times relevant to this Indictment:

INTRODUCTION

1. From in or about February 2010 through in or about the present, the defendants set forth below, together with others, engaged in an international computer hacking and fraudulent securities trading scheme whereby they: (a) hacked into the computer networks of Marketwired L.P., PR Newswire Association LLC, and Business Wire (collectively, the "Victim Newswires"); (b) stole confidential press releases containing material nonpublic information from the Victim Newswires' internal computer networks prior to their public release (the "Stolen Releases"); and (c) traded ahead of the material

nonpublic information contained in the Stolen Releases before its distribution to the investing public. During the course of the scheme, the defendants accessed more than 150,000 Stolen Releases and executed profitable trades based on the material nonpublic information contained in the Stolen Releases. In total, the scheme generated more than $30 million in illicit trading profits.

Relevant Individuals and Entities

2. Defendant IVAN TURCHYNOV, a/k/a "Ivan Turchinov," a/k/a "Ivan Turchinoff," a/k/a "Vladimir Gopienko," a/k/a "DSU," was a computer hacker who resided in Ukraine.

3. Defendant OLEKSANDR IEREMENKO, a/k/a "Aleksandr Eremenko," a/k/a "Zlom," a/k/a "Lamarez," was a computer hacker who resided in Ukraine.

4. Defendant ARKADIY DUBOVOY resided in or around Alpharetta, Georgia, and engaged in securities trading.

5. Defendant IGOR DUBOVOY resided in or around Alpharetta, Georgia, and engaged in securities trading. Defendant IGOR DUBOVOY was defendant ARKADIY DUBOVOY's son.

6. Defendant PAVEL DUBOVOY resided in or around Ukraine, and engaged in securities trading. Defendant PAVEL DUBOVOY was related to defendants ARKADIY DUBOVOY and IGOR DUBOVOY.

7. Co-Conspirator #1 ("CC-1"), a co-conspirator not named as a defendant herein, resided in or around Alpharetta, Georgia, and engaged in securities trading.

8. Co-Conspirator #2 ("CC-2"), a co-conspirator not named as a defendant herein, resided in or around Glenn Mills, Pennsylvania, engaged in securities trading, and was formerly a broker-dealer registered with the United States Securities and Exchange Commission ("SEC").

9. Co-Conspirator #3 ("CC-3"), a co-conspirator not named as a defendant herein, resided in or around Brooklyn, New York, and in Ukraine, engaged in securities trading, and was formerly a broker-dealer registered with the SEC.

10. Co-Conspirator #4 ("CC-4"), a co-conspirator not named as a defendant herein, resided in or around Suwanee, Georgia, and engaged in securities trading.

11. At various times relevant to this Indictment, defendants ARKADIY DUBOVOY, IGOR DUBOVOY, and PAVEL DUBOVOY (collectively, the "Trader Defendants"), and their co-conspirators, either opened, maintained, controlled, benefitted from, or were designated as authorized traders, on a number of brokerage accounts in which the trades discussed below were executed. Indeed, at various times relevant to this Indictment, certain of the Trader Defendants shared login credentials to the brokerage accounts with each other and with other co-conspirators, thereby permitting trades to be executed by multiple individuals in multiple accounts in furtherance of the scheme.

12. Tanigold Assets LTD was an overseas entity associated with defendant PAVEL DUBOVOY, which maintained a foreign bank account that was used by the Trader Defendants to send a portion of the proceeds of the

scheme described herein to, among others, defendants TURCHYNOV and IEREMENKO (collectively, the "Hacker Defendants").

13. "Shell Company #1" and "Shell Company #2" were overseas entities, which maintained foreign bank accounts, that were used by the Hacker Defendants to receive proceeds from the scheme described herein.

14. The Victim Newswires included the following entities, including any predecessor entities: Marketwired L.P. ("Marketwired"), which was headquartered in or around Toronto, Canada; PR Newswire Association LLC ("PRN"), which was headquartered in or around New York, New York, and maintained and utilized computer servers located in the District of New Jersey that were affected by the unlawful activity discussed below; and Business Wire, which was headquartered in or around San Francisco, California.

15. The Victim Newswires were in the business of, among other things, issuing press releases on behalf of publicly traded companies (the "Issuers"), including, among others: Aéropostale, Inc.; Align Technology, Inc.; AllianceBernstein Holding, L.P.; Allstate Corp.; Bank of America Corp.; Boeing Co.; Caterpillar, Inc.; Clorox Co.; Deere & Co.; Delta Airlines, Inc.; Domino's Pizza, Inc.; Dreamworks Animation SKG, Inc.; E.I. DuPont de Nemours & Co.; Edwards Lifesciences Corp.; Express Scripts Holding Co.; Ford Motor Co.; Hain Celestial Group, Inc.; Hewlett Packard Co.; Home Depot, Inc.; Honeywell International, Inc.; Kroger Company; Netflix, Inc.; Northrop Grumman Corp.; Nvidia Corp.; Panera Bread Co.; Smith & Wesson Holding Corp.; Texas Instruments, Inc.; Verisign, Inc.; and Viacom, Inc.

16. Generally, the Victim Newswires maintained contractual relationships with Issuers, pursuant to which Issuers provided confidential press releases to the Victim Newswires, which maintained them on their computer servers for a period of time until their distribution to the public. The Victim Newswires finalized and released the press releases to the public at the direction of, or in consultation with, the Issuers. The press releases typically contained material nonpublic information concerning, among other things, the Issuers' financial performance, quarterly earnings, year-end earnings, and potential mergers or acquisitions involving the Issuers. As a result, maintaining the confidentiality of this information prior to its public release was critical to the operations of the Victim Newswires and to the Issuers. Indeed, the Victim Newswires and the Issuers had the right to control the use of the confidential and economically valuable business information contained in the press releases, including determining when and how the information would be disclosed to the investing public. Accordingly, the Victim Newswires maintained press releases on restricted, nonpublic servers prior to distributing the final press releases.

17. "Employee #1" and "Employee #2" were employees of Business Wire.

18. The New York Stock Exchange, or "NYSE," was the largest stock exchange in the United States based on market capitalization. By in or about the first quarter of 2011, NYSE's trade processing and data services were performed at its United States data center in or around Mahwah, New Jersey.

19. The NASDAQ Stock Market, or "NASDAQ," was the largest electronic equity securities trading market in the United States and was the second largest equities-based exchange in the world based on market capitalization. NASDAQ did not have a central trading floor. Instead, it relied on computer servers to facilitate all trading activity. Since at least in or about 2009, NASDAQ maintained computer servers in or around Carteret, New Jersey.

20. Knight Capital Group, Inc. ("Knight") was engaged in the business of, among other things, market making and the electronic execution of trades involving securities traded on the NYSE and NASDAQ. Knight's headquarters were located in or around Jersey City, New Jersey, and its computer servers were also located in the District of New Jersey.

21. Direct Edge ("EDGX") was a registered national securities exchange that operated an all-electronic exchange. EDGX was located in or around Jersey City, New Jersey, and maintained servers at a data center located in or around Secaucus, New Jersey.

22. At all times relevant to this Indictment, the trades described below were executed through NYSE, NASDAQ, EDGX, or Knight servers located in the District of New Jersey.

Relevant Hacking Terms

23. "Brute Force Attacks" or "bruting" referred to decrypting data by running programs that systematically checked all possible passwords until the correct password was revealed. Among other things, this methodology could be

used to decrypt "password hashes," which were strings of encrypted data generated when a password was passed through an encryption algorithm. Passwords for network accounts were often stored on networks as password hashes as a security measure.

24. "Internet Protocol ('IP') addresses" were unique numeric addresses assigned to every Internet connection. Every device connected to the Internet was assigned an IP address in order to send and receive communications with other devices or services available on the Internet.

25. "Malware" was malicious software programmed to, among other things, gain unauthorized access to computers; identify, store, and export information from hacked computers; and to evade detection of intrusions by anti-virus programs and other security features running on those computers.

26. "Phishing" referred to an attempt to gain unauthorized access to a computer or computers by sending an email that appeared to be a legitimate communication from a trustworthy source, but contained malware or a link to download malware.

27. "Reverse shells" were a specific type of malware designed to initiate a connection to an external computer from within a hacked computer network.

28. "Structured Query Language" or "SQL" was a computer programming language designed to retrieve and manage data in computer databases.

29. "SQL Injection Attacks" were methods of hacking into and gaining unauthorized access to computers connected to the Internet using a series of SQL instructions.

Relevant Securities Terms

30. A "put" referred to an option contract giving the purchaser of that contract the right to sell a certain number of shares in a security at a specific price within a specified time. Puts allowed an investor to profit from a decrease in a security's market price.

31. A "call" referred to an option contract giving the purchaser of that contract the right to purchase a certain number of shares in a security at a specific price within a specified time. Calls allowed an investor to profit from an increase in a security's market price.

32. "Shorting" stock referred to the practice of borrowing shares for a specified time from a lender, typically a broker-dealer, and then selling those shares to another buyer at the current market price. Shorting allowed an investor to profit from a decrease in a security's market price because the investor would typically purchase the stock at a lower price at a later date to return to the broker-dealer from whom the investor borrowed the stock. The purchase of stock to return to the broker-dealer from whom the investor borrowed the stock was known as "covering a short position."

33. A "short" position referred to the practice of shorting stock, or purchasing a put option, with the expectation that the market price for the underlying security would decrease in value.

34. A "long" position referred to the purchase of a security or call option with the expectation that the market price for the underlying security would increase in value.

35. "Closing out" referred to the monetization of a particular position. Closing a long position in a security entailed selling the purchased security, or in the case of a call option, selling the security purchased pursuant to the option contract. Closing a short position entailed buying back and returning the borrowed security, or in the case of a put option, selling the security pursuant to the option contract.

Overview of the Scheme

36. From in or about February 2010 through in or about the present, the Hacker Defendants and others gained unauthorized access into the computer networks of the Victim Newswires and stole confidential press releases containing material nonpublic information prior to their public release. The Hacker Defendants then shared the Stolen Releases with, among others, the Trader Defendants using overseas computer servers. The Trader Defendants traded on the material nonpublic information contained in the Stolen Releases prior to their distribution to the investing public. The Trader Defendants paid the Hacker Defendants for access to the servers based, in part, on a percentage of how much money the Trader Defendants made trading ahead of the information contained in the Stolen Releases.

37. In order to execute their trades before the Stolen Releases were made public, the Trader Defendants and other co-conspirators sometimes

executed trades in very short windows of time between when the Hacker Defendants illegally accessed and shared the Stolen Releases and when the press releases were disseminated to the public by the Victim Newswires, usually shortly after the close of the markets. Frequently, all of this activity occurred on the same day. Thus, as discussed more fully below, the trading data for the Trader Defendants often showed a flurry of trading activity around a Stolen Release just prior to its public release.

38. In executing the scheme, the Hacker Defendants and the Trader Defendants deprived the Victim Newswires and the Issuers of their right to control the use of the confidential and economically valuable business information contained in the Stolen Releases, including the decision of when and how the information should be disclosed to the public.

39. During the period of the scheme, the defendants named herein and their co-conspirators, including CC-1, CC-2, CC-3, and CC-4, obtained over 150,000 Stolen Releases, executed trades in advance of over approximately 800 of the Stolen Releases, and realized over $30 million in illicit trading profits.

The Intrusions into the Victim Newswires

A. Marketwired

40. From in or about February 2010 through in or about November 2013, the Hacker Defendants gained unauthorized access to press releases on the networks of Marketwired using a series of SQL Injection Attacks. Between on or about April 24, 2012 and on or about July 20, 2012 alone, defendant

TURCHYNOV sent SQL Injection Attack commands into the networks of Marketwired on at least 390 occasions.

41. The first theft of press releases from Marketwired's networks occurred at least as early as on or about February 26, 2010. After gaining access, the Hacker Defendants installed multiple reverse shells onto Marketwired's networks, which they used to facilitate their theft of data. For example, in or about May 2012, after the Hacker Defendants installed multiple reverse shells onto the networks of Marketwired, an IP address associated with defendant TURCHYNOV accessed press releases on Marketwired's servers.

42. In addition to sending SQL Injection Attack commands, in or about March 2012, the Hacker Defendants launched an intrusion into the networks of Marketwired whereby they obtained contact and credential information for Marketwired's employees, clients, and business partners. This intrusion gave the Hacker Defendants access to employee log-in credentials. The Hacker Defendants then misrepresented their identities by using these login credentials to gain access to confidential information, including press releases, located on Marketwired's networks.

43. From in or about February 2010 through in or about November 2013, the Hacker Defendants had access to the content of more than 150,000 press releases on the internal networks of Marketwired before they were released to the investing public; approximately 968 of these press releases were recovered on a laptop belonging to defendant TURCHYNOV that was seized in or about November 2012.

44. The Hacker Defendants continued to attempt to gain unauthorized access to Marketwired's networks until at least as late as in or about July 2015.

45. On or about July 13, 2015, several Marketwired employees received a phishing email with an attachment that contained a link to malware associated with an IP address ending in 75 (the "75 IP Address"). Marketwired, however, identified the email as a phishing attempt and prevented the intrusion. The phishing email was sent from an email account that was created the same day the email was sent and was created from an IP address associated with defendant IEREMENKO.

B. PRN

46. The Hacker Defendants hacked into PRN's computer servers in the District of New Jersey on the following three occasions: from in or about July 2010 through in or about January 2011; from in or about July 2011 through in or about March 2012; and from in or about January 2013 through in or about March 2013. During these intrusions, the Hacker Defendants accessed and exfiltrated more than approximately 40,000 press releases before they were publicly disseminated.

47. During the first intrusion, in or about October 2010, defendant TURCHYNOV sent several emails with attachments containing Stolen Releases exfiltrated from PRN. For example, in one email dated on or about October 28, 2010, defendant TURCHYNOV sent approximately 96 Stolen Releases exfiltrated from PRN to another individual; the subject of the email, which was

originally in Russian, read in substance and part, "fresh stuff," and the body of the email read, in substance and in part, "[a]nd if he says he does not know what this is about, tell him 'quarterly report'...."

48. On or about January 12, 2011, PRN changed its network infrastructure, which had the effect of cutting off the Hacker Defendants' access to its networks. As a result, between on or about January 12, 2011 and in or about June 2011, the Hacker Defendants increased their activities within the networks of Marketwired, where they still maintained access at the time.

49. Between in or about July 2011 and in or about March 2012, the Hacker Defendants regained access to PRN's networks and installed malware on its servers. During this same time period, the Hacker Defendants' activities on the networks of Marketwired decreased, and they shifted their focus to PRN's networks.

50. Between on or about March 9, 2012 and on or about March 13, 2012, PRN identified and removed malware that the Hacker Defendants had installed on its servers, resulting in the Hacker Defendants once again losing their unauthorized access to PRN's networks.

51. Thereafter, in an online chat in Russian dated on or about March 27, 2012, another individual informed defendant TURCHYNOV, in sum and substance, that they had lost access to the networks of PRN and that PRN "detected the module... and removed everything . . . ."

52. In subsequent online chats between on or about June 26, 2012 and on or about October 12, 2012, defendant IEREMENKO discussed with multiple other individuals the Hacker Defendants' ongoing attempts to regain access to the networks of PRN. Thereafter, on or about October 10, 2012, defendant IEREMENKO sent an online chat message in Russian stating "I'm hacking prnewswire.com."

53. Between on or about January 25, 2013 and on or about March 1, 2013, the Hacker Defendants regained unauthorized access to the networks of PRN. On or about March 1, 2013, however, PRN detected the intrusion and once again blocked the Hacker Defendants' unauthorized access to its networks. Consistent with their prior patterns, after losing access to PRN's networks, the Hacker Defendants increased their activities on the networks of Marketwired.

54. The Hacker Defendants continued to attempt to gain unauthorized access to PRN's networks until at least as late as in or about February 2014.

55. During the periods of unauthorized access discussed in paragraphs 46 through 54 above, the Hacker Defendants had access to over 150,000 nonpublic press releases from the internal networks of PRN, approximately 200 of which were recovered from a laptop seized from defendant TURCHYNOV in or about November 2012.

C. Business Wire

56. From in or about March 2012 through in or about June 2012, the Hacker Defendants hacked into Business Wire and stole the login credentials of

a number of Business Wire's employees. The Hacker Defendants misrepresented their identities by using these login credentials to gain unauthorized access to Business Wire's networks in an effort to steal press releases from Business Wire prior to their public distribution.

57. In an online chat dated on or about October 27, 2010, defendant TURCHYNOV stated to another individual in Russian, in sum and substance, that he intended to add Business Wire to his collection of hacked "news" companies. The other individual questioned whether co-conspirators, including defendant TURCHYNOV, were selling the "news" too cheaply. Defendant TURCHYNOV agreed and stated that, in the beginning, they had to sell the Stolen Releases for whatever was offered for them.

58. In another online chat dated on or about March 25, 2012, defendant IEREMENKO told defendant TURCHYNOV that the login credentials of approximately fifteen Business Wire employees had been "bruted."

59. In an online chat dated on or about March 26, 2012, defendant IEREMENKO sent defendant TURCHYNOV a link to malware placed within the networks of Business Wire.

60. Defendant IEREMENKO maintained on his laptop a file containing approximately 219 user identifications and associated hashed passwords for users of Business Wire's computer networks that was last modified on or about March 24, 2012. The laptop also contained multiple variants of the malware that had been installed on Business Wire's networks. In addition, the internet history on one of defendant TURCHYNOV's laptops showed that between on or

about March 26, 2012 and on or about June 5, 2012, defendant TURCHYNOV accessed malware that had been installed on Business Wire's networks at least 39 times.

61. Defendant IEREMENKO maintained on his laptop a file containing approximately 41 user identifications and associated hashed passwords for users of Business Wire's computer networks that was last modified on or about March 28, 2012. The word "GOOD" appeared next to some of the user identifications and passwords. A number of the user identifications and associated hashed passwords also included a brief note about the user as well as annotations such as "ADMIN" or "REG USER," which reflected the level of access associated with each compromised user identification and password. "ADMIN," for example, signified that that the user had administrative rights and a greater level of network access.

62. Both the March 24th and the March 28th files recovered from defendant IEREMENKO's laptop contained the user identifications and passwords of, among others, Employee #1 and Employee #2. On or about March 27, 2012, defendant IEREMENKO sent the login credentials for Employee #2 to defendant TURCHYNOV in an internet chat. On or about March 31, 2012, defendant IEREMENKO sent the login credentials for Employee #1 to defendant TURCHYNOV in an internet chat. The internet history recovered from defendant TURCHYNOV's laptop showed that defendant TURCHYNOV accessed Business Wire's computer networks using the login

credentials of Employee #2 shortly after he received them from defendant IEREMENKO.

63. In addition, over 150 files related to Business Wire were recovered from defendant IEREMENKO's laptop, including a spreadsheet listing the positions and contact information for over 500 Business Wire employees.

64. From in or about September 2014 through at least as late as in or about May 2015, the Hacker Defendants regained entry into Business Wire's networks and successfully obtained Stolen Releases which the Trader Defendants used in furtherance of the scheme described herein. Business Wire identified a number of IP addresses associated with this intrusion and the exfiltration of Stolen Releases during this period, including the 75 IP address associated with the July 13, 2015 phishing attempt directed at Marketwired discussed above.

The Stolen Release Server

65. The Hacker Defendants shared the Stolen Releases by, among other methods, creating servers where the Trader Defendants and others could quickly access and download the Stolen Releases before they were publicly disseminated by the Victim Newswires. As more fully set forth below, the Trader Defendants compensated the Hacker Defendants, in part, based on the profits the Trader Defendants realized by trading ahead of the Stolen Releases.

66. In order to facilitate its use, the Hacker Defendants created a video tutorial on how to access and use one of the servers they used to share the Stolen Releases (the "Stolen Release Server"). For example, on or about

October 25, 2010, defendant TURCHYNOV sent an email to another individual containing the video tutorial. The body of the email contained only the words "to watch" in Russian. The video attachment, entitled "readme.avi," was a Russian-language video that showed the desktop interface of a computer screen as the user of that computer performed the necessary steps to access the Stolen Releases on the Stolen Release Server. The user in the video typed text instructions on the screen, and the video showed, among other things, a web-based server where individuals with access to the server could select and download press releases prior to their public distribution by the Victim Newswires. The IP Address for the Stolen Release Server, which ended in 98 (the "98 IP Address"), and several press releases could be seen in the video. The typed instructions, which were in Russian, translated as follows:

> This is what the administrative panel with files looks like. On the left is a list of files beginning with the last one requested. By selecting the files we select what to download. After selecting the files, we press download. The admin panel will itself download and pack up the files. For now, that's it. Log-in data will be sent to the email you leave.

67. The Stolen Release Server was shared among the Trader Defendants through, among others, defendant PAVEL DUBOVOY. For example, on or about November 26, 2010, defendant PAVEL DUBOVOY sent CC-1 an email, the subject line of which contained the word "stocks" in Russian. Attached to the email was a file entitled "READ_ME!!!.txt," which contained a link to the 98 IP Address associated with the Stolen Release Server and login credentials for the site and additional written instructions. The

written instructions described much of what can be seen in the video tutorial originally provided by defendant TURCHYNOV in the email described above in paragraph 66. Specifically, the instructions described a web-based server that contained a list of "Documents." The user was instructed to choose a file to download by clicking the box next to the document name. According to the instructions, an "Archives" panel then showed the downloaded files. The following suggestion appeared at the end of the instructions, in Russian, and has been translated as follows:

> On the server, logs are not maintained, plus the entire file system is encrypted through an AES algorithm key 4096, but I still highly recommend using a proxy, VPN, or another way to conceal your IP and other information leaving the network from your provider. I can advise on this question.

The above instructions suggested, in sum and substance, that users should conceal their IP address when accessing the Stolen Release Server as a precaution to avoid detection.

68. On or about December 6, 2010, CC-1 sent an email to another individual containing the same instructions to access the Stolen Release Server that CC-1 had previously received from defendant PAVEL DUBOVOY on or about November 26, 2010.

69. On or about December 16, 2010, CC-1 sent another email to the same individual containing a collection of sample Stolen Releases.

70. On or about December 16, 2010, CC-1 sent an email to the same individual, the subject line of which read "address" and the body of which

contained a link to the Stolen Release Server. On that same date, defendant ARKADIY DUBOVOY opened a brokerage account.

71. On or about January 20, 2011, defendant PAVEL DUBOVOY created a draft of an email, which was stored in the "Drafts" folder of his email account and which contained a link to the 98 IP Address of the Stolen Release Server in the subject line of the email. The body of the email contained a link to the Stolen Release Server along with login credentials. The password contained in the email was one frequently used by defendant TURCHYNOV.

The Trader Defendants Provided Shopping Lists to the Hacker Defendants

72. On or about October 12, 2011, defendant PAVEL DUBOVOY sent an email to another individual suggesting that he and the Trader Defendants had not received advance copies of press releases that had been issued earlier that week. Attached to the email was a list of Issuers that were scheduled to make announcements in the upcoming two weeks, and defendant PAVEL DUBOVOY indicated in the email that the list – which was essentially a shopping list for the Hacker Defendants to use as they traversed the Victim Newswires' networks – could help in obtaining Stolen Releases in the upcoming two weeks.

73. On or about October 8, 2013, defendant PAVEL DUBOVOY sent an email to defendant ARKADIY DUBOVOY containing another shopping list of desired upcoming press releases for publicly traded companies. The letter "M" was handwritten at the top of the list, and it contained several upcoming Marketwired press releases. After the shopping list was sent, the Trader

Defendants and their co-conspirators traded ahead of several of the press releases referred to in the list, including, as discussed in greater detail below, Align Technology, Inc.'s press release on or about October 17, 2013; and Panera Bread Co.'s press release on or about October 22, 2013.

74. On or about January 3, 2014, defendant PAVEL DUBOVOY sent an email to defendant ARKADIY DUBOVOY containing a shopping list of desired upcoming press releases for publicly traded companies. The shopping list had a column in which the letters "PRN" or "MWR" appeared next to the Issuers' name and the anticipated date of the release, indicating whether the nonpublic release could be found on PRN or on Marketwired's servers.

The Defendants Realized Massive Profits by Trading Ahead of the Stolen Releases

75. During the time period relevant to this Indictment, the Trader Defendants' activities largely shadowed the Hacker Defendants' capabilities to exfiltrate Stolen Releases from the internal networks of the Victim Newswires.

A. The Trader Defendants' Trading Patterns

76. For example, from in or about February 2010 through in or about November 2013, the Hacker Defendants had access to the internal networks of Marketwired. Beginning in or about July 2010 and continuing through in or about January 2011, however, the Hacker Defendants also gained access into the internal networks of PRN. During that time period, the Trader Defendants and their co-conspirators traded almost exclusively ahead of Stolen Releases

from PRN, and their trading activities in relation to Issuers that used Marketwired's services decreased.

77. On or about January 12, 2011, the Hacker Defendants lost access to the network infrastructure of PRN, and the Trader Defendants and their co-conspirators reverted back to trading ahead of Stolen Releases from Marketwired, where the Hacker Defendants still maintained access at the time. When the Hacker Defendants regained access to PRN from in or about July 2011 through in or about March 2012, the Trader Defendants and their co-conspirators again traded ahead of Stolen Releases from PRN, and their activities relating to Marketwired decreased.

78. The patterns described above repeated themselves when, in or about March 2012, PRN once again blocked the Hacker Defendants' access to their internal networks. Accordingly, from in or about March 2012 through in or about January 2013, the Trader Defendants and their co-conspirators ceased trading ahead of press releases from PRN, and resumed trading ahead of Stolen Releases from Marketwired, where the Hacker Defendants still maintained access at the time.

79. Predictably, from in or about January 2013 through in or about March 2013, during the time period when the Hacker Defendants regained access to the internal networks of PRN for the final time, the Trader Defendants and their co-conspirators nearly exclusively traded ahead of Stolen Releases from PRN, and their trading activities based on Stolen Releases obtained from Marketwired decreased.

B. Selected Examples of Illicit Trading Activity

80. By accessing Stolen Releases, the Trader Defendants and their co-conspirators obtained material nonpublic information concerning a number of publicly traded companies that had been stolen by the Hacker Defendants, and then executed trades on the basis of that information before its distribution to the public, including the examples outlined below.

Caterpillar, Inc. ("CAT") – October 21–24, 2011

81. On or about October 21, 2011, Caterpillar, Inc., which was a publicly traded company whose stock was listed on the NYSE stock exchange under the ticker symbol "CAT," submitted a press release to PRN for distribution to the investing public. In the press release, CAT announced that its third-quarter profit after taxes had increased by 27% in comparison to the prior year. The press release was not distributed to the public by PRN until before the opening of the market on or about October 24, 2011.

82. On or about October 21, 2011, after CAT sent its press release to PRN, but prior to its public release before the opening of the market on or about October 24, 2011, the Trader Defendants and their co-conspirators executed a number of trades involving buying both shares of CAT and options to purchase shares of CAT in multiple brokerage accounts. In total, the Trader Defendants and their co-conspirators purchased more than approximately $5.9 million worth of shares and options of CAT during this time period. This trading activity included, among others, a trade to purchase approximately 3,800 shares of CAT, which trade was executed through EDGX and in a

brokerage account ending in 0365 maintained in the name of defendant ARKADIY DUBOVOY (the "ARKADIY DUBOVOY 0365 Account").

83. On or about October 24, 2011, following the public release of the press release described above, the price of CAT increased. By on or about October 24, 2011, the Trader Defendants and their co-conspirators closed out their positions for a profit of more than approximately $648,000.

CAT– January 25–26, 2012

84. On or about January 25, 2012, CAT submitted a press release to PRN for distribution to the investing public. In the press release, CAT announced that its profit after tax increased 36% over the prior year. The press release was not distributed to the public by PRN until before the opening of the market on or about January 26, 2012.

85. On or about January 25, 2012, after CAT sent its press release to PRN, but prior to its public release before the opening of the market on the next day, the Trader Defendants and their co-conspirators executed a number of trades involving buying both shares of CAT and call options to purchase CAT shares in multiple brokerage accounts. In total, the Trader Defendants and their co-conspirators purchased more than approximately $8.3 million worth of CAT shares and options during this time period. This trading activity included, among others, a trade to purchase approximately 600 shares of CAT, which trade was executed through Knight and in a brokerage account ending in 0584 maintained in the name of defendant ARKADIY DUBOVOY (the "ARKADIY DUBOVOY 0548 Account").

86. On or about January 26, 2012, following the public release of the press release described above, the price of CAT increased. By on or about January 26, 2012, the Trader Defendants and their co-conspirators closed out their positions for a profit of more than approximately $1 million.

Acme Packet, Inc. ("APKT") – July 25–27, 2012

87. On or about July 25, 2012, Acme Packet, Inc., which was a publicly traded company whose stock was listed on the NASDAQ stock exchange under the ticker symbol "APKT," submitted a press release to Marketwired for distribution to the investing public. In the press release, APKT announced that its second quarter revenue went down approximately 15.5% and that its earnings per share went down approximately 55% in comparison to the previous year. The press release was not distributed to the public by Marketwired until after the close of the market on or about July 26, 2012.

88. On or about July 26, 2012, after APKT sent its press release to Marketwired, but prior to its public release following the close of the market that day, the Trader Defendants and their co-conspirators executed a number of trades involving APKT in multiple brokerage accounts. The Trader Defendants and their co-conspirators shorted and purchased put options of APKT. The total amount spent by the Trader Defendants in order to establish these positions was more than approximately $4.3 million. This trading activity included, among others, a trade to short approximately 2,000 shares of APKT, which trade was executed through EDGX and in a brokerage account

ending in 6987 maintained in the name of defendant ARKADIY DUBOVOY (the "ARKADIY DUBOVOY 6987 Account").

89. On or about July 27, 2012, following the public release of the press release described above, the price of APKT decreased. By on or about July 27, 2012, the Trader Defendants and their co-conspirators closed out their short positions for a profit of more than approximately $685,000.

Edwards Lifesciences ("EW") – April 23–24, 2013

90. On or about April 23, 2013, Edwards Lifesciences, which was a publicly traded company whose stock was listed on the NYSE stock exchange under the ticker symbol "EW," submitted a press release to Marketwired. In the press release, EW announced that it was lowering its guidance for the next quarter. The press release was not distributed to the public by Marketwired until after the close of the market on or about April 23, 2013.

91. On or about April 23, 2013, shortly after EW sent its press release to Marketwired, but prior to its public release following the close of the market that day, the Trader Defendants and their co-conspirators executed a number of trades involving EW in multiple brokerage accounts. The Trader Defendants and their co-conspirators shorted and purchased put options of EW. The total amount spent by the Trader Defendants in order to establish these positions was more than approximately $3.6 million. This trading activity included, among others, a trade to short approximately 9,500 shares of EW, which trade was executed through Knight and in a brokerage account ending in 6216

maintained in the name of defendant ARKADIY DUBOVOY (the "ARKADIY DUBOVOY 6216 Account").

92. On or about April 24, 2013, following the public release of the press release described above, the price of EW decreased. By on or about April 24, 2013, the Trader Defendants and their co-conspirators closed out a number of the positions that they had established the previous day for a profit of more than approximately $844,000.

Verisign, Inc. ("VRSN") – April 25–26, 2013

93. On or about April 25, 2013, Verisign, which was a publicly traded company whose stock was listed on the NASDAQ stock exchange under the ticker symbol "VRSN," submitted a press release to Marketwired. In the press release, VRSN announced, among other things, 15% year-over-year growth, beating analysts' expectations. The press release was not distributed to the public by Marketwired until after the close of the market on or about April 25, 2013.

94. On or about April 25, 2013, shortly after VRSN sent its press release to Marketwired, but prior to its public release following the close of the market that day, the Trader Defendants and their co-conspirators executed a number of trades involving VRSN in multiple brokerage accounts. Specifically, the Trader Defendants and their co-conspirators purchased more than approximately $2.4 million worth of VRSN shares during this period. This trading activity included, among others, a trade to purchase approximately 700

shares of VRSN, which trade was executed through Knight and in the ARKADIY DUBOVOY 6987 Account.

95. On or about April 25, 2013, after the close of the market, Marketwired distributed the VRSN press release to the public. Despite the positive news in the press release, the price of VRSN unexpectedly decreased on the day following the announcement.

96. In response to the unexpected decrease in the VRSN stock price, on or about April 26, 2013, defendant IGOR DUBOVOY sent an email to CC-2 which read in part: "Arkadiy asked me to sell all the stocks if you do not have Internet can you please let me know if I should do it or if you have the service to do it." Shortly thereafter, on or about April 26, 2013, defendant IGOR DUBOVOY closed out the Trader Defendants' and their co-conspirators' positions as described in paragraph 94 above for a loss of approximately $114,038. Defendant IGOR DUBOVOY then sent CC-2 another email which read as follows: "I already sold everything and just saw your email not sure if i sold it the way you had it planned." CC-2 responded in an email to defendant IGOR DUBOVOY, which read as follows: "its ok . . . not the last day . . . it was strange anyway . . . got the numbers right . . . reaction mixed."

Align Technology, Inc. ("ALGN") – October 17–18, 2013

97. On or about October 17, 2013, Align Technology, Inc., which was a publicly traded company whose stock was listed on the NASDAQ stock exchange under the ticker symbol "ALGN," submitted a press release to Marketwired. In the press release, ALGN announced that net revenues were up

20.5% year-over-year and that earnings per share increased to $0.42 from $0.00 year-over-year. The press release was not distributed to the public by Marketwired until after the close of the market on that same date.

98. On or about October 17, 2013, shortly after ALGN sent its press release to Marketwired, but prior to its public release following the close of the market that day, the Trader Defendants and their co-conspirators executed a number of trades involving ALGN in multiple brokerage accounts. Specifically, the Trader Defendants and their co-conspirators purchased more than approximately $8.7 million worth of ALGN shares during this time period. This trading activity included, among others, a trade to purchase approximately 2,100 shares of ALGN, which trade was executed through Knight and in the ARKADIY DUBOVOY 6987 Account.

99. On or about October 18, 2013, following the public release of the press release described above, the price of ALGN increased. By on or about October 18, 2013, the Trader Defendants and their co-conspirators closed out the positions they had established the previous day for a total profit of more than approximately $1.45 million.

Panera Bread Co. ("PNRA") – October 22–23, 2013

100. On or about October 22, 2013, Panera Bread, which was a publicly traded company whose stock was listed on the NASDAQ stock exchange under the ticker symbol "PNRA," submitted a press release to Marketwired. In the press release, PNRA announced that it was revising its earning guidance downward for the fourth quarter of 2013. The press release was not

distributed to the public by Marketwired until after the close of the market on that same date.

101. On or about October 22, 2013, shortly after PNRA sent its press release to Marketwired, but prior to its public release following the close of the market that day, the Trader Defendants and their co-conspirators shorted and purchased put options of PNRA. The total amount spent by the Trader Defendants in order to establish these positions was more than approximately $17 million. This trading activity included, among others, the purchase of approximately 300 shares of PNRA, which trade was executed through Knight and covered the short sale of PNRA in the ARKADIY DUBOVOY 0584 Account.

102. On or about October 23, 2013, following the public release of the press release described above, the price of PNRA decreased. By on or about October 23, 2013, however, the Trader Defendants and their co-conspirators closed out several of the positions they had taken the previous day for a profit of more than approximately $1 million.

The Defendants Used Foreign Shell Companies to Share the Illegal Trading Profits

103. The Hacker Defendants profited from the Stolen Releases by, among other things, sharing in the illegal trading profits realized by the Trader Defendants and their co-conspirators. On or about April 21, 2011, in an online chat in Russian, defendant TURCHYNOV told another individual, in sum and substance, that in exchange for access to the Stolen Releases through "the more or less convenient web interface," users of the information paid a

percentage of their monthly or "seasonal" profits. He added: "if you get really high with time you pay a fixed amount of dough a month."

104. A portion of the illegal proceeds discussed above was filtered from the Trader Defendants and their co-conspirators to the Hacker Defendants through foreign shell companies.

105. In multiple chats in Russian dated between on or about June 6, 2011 and on or about December 1, 2011, another individual asked defendant TURCHYNOV where money should be sent. In response, on numerous occasions, defendant TURCHYNOV told the individual to have the money sent to various bank accounts, including accounts located in Estonia and Macau. After payments were sent to the accounts specified by defendant TURCHYNOV, the individual sent via online chats (sometimes at defendant TURCHYNOV's express request) a confirmation of the payment.

106. In addition, in a chat dated on or about June 6, 2011, defendant TURCHYNOV sent the individual discussed in paragraph 105 bank account information for Shell Company #1. Approximately three days later, on or about June 9, 2011, defendant PAVEL DUBOVOY received an email containing the bank account information for Shell Company #1.

107. Similarly, in chats dated on or about December 1, 2011 and on or about December 3, 2011, defendant TURCHYNOV told a co-conspirator to use Shell Company #2. Thereafter, on or about February 3, 2012, defendant PAVEL DUBOVOY received an email containing bank account information for Shell Company #2. Approximately five-and-a-half hours later that same day,

defendant PAVEL DUBOVOY emailed a co-conspirator confirmation of a $65,000 wire transfer from his entity – Tanigold Assets LTD – to Shell Company #2.

108. On or about that same date, defendant PAVEL DUBOVOY sent an email in Russian to an email address associated with defendant ARKADIY DUBOVOY itemizing sums of money received and spent between on or about January 27, 2012 and on or about February 3, 2012. The email specifically listed a $95,000 payment to Shell Company #2 next to the word "guys" written in parentheses.

109. To monitor the profits being derived from the illegal trading activity described herein, defendant TURCHYNOV sometimes checked on certain of the trading accounts used by the Trader Defendants. For example, on or about July 20, 2011, defendant PAVEL DUBOVOY sent an email to another individual containing the login credentials for one of the trading accounts used by the Trader Defendants. The next day, on or about July 21, 2011, defendant TURCHYNOV logged into that trading account (from the same IP address that was used to hack into the computer networks of Marketwired and PRN).

The Trader Defendants' Efforts to Expand the Securities Fraud Scheme

110. During the course of the scheme described herein, the Trader Defendants also explored additional opportunities to commit securities fraud. For example, on or about January 19, 2013, defendant PAVEL DUBOVOY received an email from another individual, which email was subsequently shared with defendant ARKADIY DUBOVOY and CC-2. The email described a

"proprietary trading business" that involved a "special daytrading strategy[.]" The email further stated that the "strategy . . . never los[t] money in the twelve months of 2012[.]" The email offered a description of the "trading strategy," and referred to an attached video showing the "strategy" in action. The email and video essentially described a fraudulent securities trading practice known as "layering" or "spoofing," pursuant to which traders placed non-bona fide orders to buy or sell securities and then quickly canceled those orders before they were executed in order to trick others to execute against them. If successful, traders engaged in such schemes could artificially move the price of securities up or down and profit from the artificial price movements through trades they placed in other accounts they controlled.

Count One
(Conspiracy to Commit Wire Fraud)

112. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

The Conspiracy

113. From in or about February 2010 through in or about the present, in Bergen, Hudson, and Middlesex Counties, in the District of New Jersey and elsewhere, defendants

IVAN TURCHYNOV,
a/k/a "Ivan Turchinov,"
a/k/a "Ivan Turchinoff,"
a/k/a "Vladimir Gopienko"
a/k/a "DSU,"
OLEKSANDR IEREMENKO,
a/k/a "Aleksandr Eremenko,"
a/k/a "Zlom,"
a/k/a "Lamarez,"
ARKADIY DUBOVOY,
IGOR DUBOVOY, and
PAVEL DUBOVOY

did knowingly and intentionally conspire and agree with each other and others to devise a scheme and artifice to defraud the Victim Newswires and the Issuers, and to obtain money and property, including the confidential business information of the Victim Newswires and the Issuers, by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and

foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

Object of the Conspiracy

114. It was the object of the conspiracy for defendants TURCHYNOV, IEREMENKO, ARKADIY DUBOVOY, IGOR DUBOVOY, PAVEL DUBOVOY and others, to obtain money and property by means of fraudulently obtaining confidential business information from the Victim Newswires and the Issuers, namely unreleased press releases containing material nonpublic information concerning publicly traded companies – the Stolen Releases – and trading upon the material nonpublic information contained in the Stolen Releases ahead of its public distribution, thereby realizing and sharing in the proceeds of the profitable illegal trading.

Manner and Means of the Conspiracy

115. It was part of the conspiracy that the Hacker Defendants gained unauthorized access to the computer networks of the Victim Newswires by employing a variety of hacking methods, including the use of stolen login credentials, SQL Injection Attacks, and Brute Force Attacks. In some cases, the Hacker Defendants illegally obtained the contact and login credential information for employees, clients, and business partners of the Victim Newswires, to gain unauthorized access to the Victim Newswires' networks. By employing these and other hacking methods, the Hacker Defendants misrepresented their identities in order to gain access to information on the

internal networks of the Victim Newswires that was otherwise off limits to them.

116. It was further part of the conspiracy that after gaining unauthorized access to the computer networks of the Victim Newswires, the Hacker Defendants exfiltrated Stolen Releases containing confidential business information from those networks.

117. It was further part of the conspiracy that the Hacker Defendants exfiltrated the Stolen Releases to servers they controlled, including the Stolen Release Server.

118. It was further part of the conspiracy that the Hacker Defendants provided access to the Stolen Release Server and the Stolen Releases contained thereon to, among others, the Trader Defendants.

119. It was further part of the conspiracy that the Trader Defendants and others executed profitable trades in brokerage accounts they controlled by trading ahead of the material nonpublic information contained in the Stolen Releases.

120. It was further part of the conspiracy that the Trader Defendants and others sent the Hacker Defendants a portion of the proceeds from their profitable trading using, among other methods, several shell companies.

121. It was further part of the conspiracy that using the means and methods described above, the conspiracy generated in excess of approximately $30 million in illicit trading profits.

In violation of Title 18, United States Code, Section 1349.

Counts Two through Eight
(Wire Fraud)

122. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

123. On or about the dates set forth below, in Bergen, Hudson, and Middlesex Counties, in the District of New Jersey and elsewhere, defendants

IVAN TURCHYNOV,
a/k/a "Ivan Turchinov,"
a/k/a "Ivan Turchinoff,"
a/k/a "Vladimir Gopienko"
a/k/a "DSU,"
OLEKSANDR IEREMENKO,
a/k/a "Aleksandr Eremenko,"
a/k/a "Zlom,"
a/k/a "Lamarez,"
ARKADIY DUBOVOY,
IGOR DUBOVOY, and
PAVEL DUBOVOY

did knowingly and intentionally devise a scheme and artifice to defraud the Victim Newswires and the Issuers, and to obtain money and property, including the confidential business information of the Victim Newswires and the Issuers, by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing and attempting to execute such scheme and artifice to defraud, did knowingly transmit and cause to be transmitted by means of wire communications in

interstate and foreign commerce to New Jersey, certain writings, signs, signals, and sounds, namely the specified trades described below, each constituting a separate count of this Indictment:

Count	Approximate Date	Description
Two	October 21, 2011	Purchase of approximately 3,800 shares of CAT in the ARKADIY DUBOVOY 0365 Account
Three	January 25, 2012	Purchase of approximately 600 shares of CAT in the ARKADIY DUBOVOY 0584 Account
Four	July 26, 2012	Short trade of approximately 2,000 shares of APKT in the ARKADIY DUBOVOY 6987 Account
Five	April 23, 2013	Short trade of approximately 9,500 shares of EW in the ARKADIY DUBOVOY 6216 Account
Six	April 25, 2013	Purchase of approximately 700 shares of VRSN in the ARKADIY DUBOVOY 6987 Account
Seven	October 17, 2013	Purchase of approximately 2,100 shares of ALGN in the ARKADIY DUBOVOY 6987 Account
Eight	October 22, 2013	Purchase of approximately 300 shares to cover short sale of PNRA in the ARKADIY DUBOVOY 0584 Account

In violation of Title 18, United States Code, Section 1343, and Title 18, United States Code, Section 2.

Count Nine
(Conspiracy to Commit Securities Fraud)

124. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

125. From in or about February 2010 through in or about the present, in Bergen, Hudson, and Middlesex Counties, in the District of New Jersey and elsewhere, defendants

IVAN TURCHYNOV,
a/k/a "Ivan Turchinov,"
a/k/a "Ivan Turchinoff,"
a/k/a "Vladimir Gopienko"
a/k/a "DSU,"
OLEKSANDR IEREMENKO,
a/k/a "Aleksandr Eremenko,"
a/k/a "Zlom,"
a/k/a "Lamarez,"
ARKADIY DUBOVOY,
IGOR DUBOVOY, and
PAVEL DUBOVOY

did willfully and knowingly conspire and agree with each other and others to, directly and indirectly, by the use of means and instrumentalities of interstate commerce, and of the mails, and of facilities of national securities exchanges, use and employ, in connection with the purchase and sale of securities, manipulative and deceptive devices and contrivances, in violation of Title 17, Code of Federal Regulations, Section 240.10b-5, by: (a) employing devices, schemes and artifices to defraud; (b) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not

misleading; and (c) engaging in acts, practices and courses of business which operated and would operate as a fraud and deceit upon persons, namely by executing and causing others to execute the securities transactions securities fraud, contrary to Title 15, United States Code, Sections 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5.

Object of the Conspiracy

126. It was the object of the conspiracy for defendants TURCHYNOV, IEREMENKO, ARKADIY DUBOVOY, IGOR DUBOVOY, PAVEL DUBOVOY and others, to enrich themselves by: (a) gaining unauthorized access to the computer networks of the Victim Newswires, including by misrepresenting their identities in order to gain access to information that was otherwise off limits to them; (b) stealing confidential business information from those networks, including press releases containing material nonpublic information concerning publicly traded companies – the Stolen Releases; (c) trading ahead of the material nonpublic information contained in the Stolen Releases; and (d) sharing in the proceeds of the profitable illegal trading.

Manner and Means of the Conspiracy

127. It was part of the conspiracy that defendants TURCHYNOV, IEREMENKO, ARKADIY DUBOVOY, IGOR DUBOVOY, PAVEL DUBOVOY and others, employed the manner and means set forth in paragraphs 114 through 120 of this Indictment.

Overt Acts

128. In furtherance of the conspiracy and to effect the unlawful objects thereof, defendants TURCHYNOV, IEREMENKO, ARKADIY DUBOVOY, IGOR DUBOVOY, PAVEL DUBOVOY and others, committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

a. From in or about July 2010 through in or about January 2011, the Hacker Defendants hacked into the computer networks of PRN.

b. From in or about July 2011 through in or about March 2012, the Hacker Defendants hacked into the computer networks of PRN.

c. Between on or about October 21, 2011 and on or about October 24, 2011, the Trader Defendants and their co-conspirators purchased approximately $4.9 million worth of shares and options of CAT.

d. Between on or about January 25, 2012 and on or about January 26, 2012, the Trader Defendants and their co-conspirators purchased approximately $7.3 million worth of shares of CAT.

e. On or about March 26, 2012, defendant IEREMENKO sent defendant TURCHYNOV a link to malware placed within the networks of Business Wire.

f. Between on or about March 26, 2012 and on or about June 5, 2012, defendant TURCHYNOV accessed malware that had been installed on Business Wire's networks approximately 39 times.

g. Between on or about April 24, 2012 and on or about July 20, 2012, defendant TURCHYNOV sent SQL Injection Attack commands into the networks of Marketwired on at least 390 occasions.

h. Between on or about July 27, 2012 and on or about July 28, 2012, the Trader Defendants and their co-conspirators shorted and purchased put options of APKT.

i. On or about October 10, 2012, defendant IEREMENKO sent an online chat message stating "I'm hacking prnewswire.com."

j. From in or about January 2013 through in or about March 2013, the Hacker Defendants hacked into the computer networks of PRN.

k. Between on or about April 23, 2013 and on or about April 24, 2013, the Trader Defendants and their co-conspirators shorted and purchased put options of EW.

l. Between on or about April 25, 2013 and on or about April 26, 2013, the Trader Defendants and their co-conspirators purchased approximately $2.2 million worth of VRSN.

m. Between on or about October 17, 2013 and on or about October 18, 2013, the Trader Defendants and their co-conspirators purchased approximately $6.7 million worth of shares of ALGN.

n. Between on or about October 22, 2013 and on or about October 23, 2013, the Trader Defendants and their co-conspirators shorted and purchased put options of PNRA.

In violation of Title 18, United States Code, Section 371.

Counts Ten through Sixteen
(Securities Fraud)

129. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

130. On or about the dates set forth below, in Bergen, Hudson, and Middlesex Counties, in the District of New Jersey and elsewhere, defendants

IVAN TURCHYNOV,
a/k/a "Ivan Turchinov,"
a/k/a "Ivan Turchinoff,"
a/k/a "Vladimir Gopienko"
a/k/a "DSU,"
OLEKSANDR IEREMENKO,
a/k/a "Aleksandr Eremenko,"
a/k/a "Zlom,"
a/k/a "Lamarez,"
ARKADIY DUBOVOY,
IGOR DUBOVOY, and
PAVEL DUBOVOY

did willfully and knowingly, directly and indirectly, by the use of means and instrumentalities of interstate commerce, and of the mails, and of facilities of national securities exchanges, would and did use and employ, in connection with the purchase and sale of securities, manipulative and deceptive devices and contrivances, in violation of Title 17, Code of Federal Regulations, Section 240.10b-5, by: (a) employing devices, schemes and artifices to defraud; (b) making untrue statements of material fact and omitting to state material facts necessary in order to make the statements made, in the light of the circumstances under which they were made, not misleading; and (c) engaging in acts, practices and courses of business which operated and would operate

as a fraud and deceit upon persons, namely by executing and causing others to execute the securities transactions described below based, in whole or in part, on material nonpublic information, each such transaction constituting a separate count of this Indictment:

Count	Approximate Date	Description
Ten	October 21, 2011	Purchase of approximately 3,800 shares of CAT in the ARKADIY DUBOVOY 0365 Account
Eleven	January 25, 2012	Purchase of approximately 600 shares of CAT in the ARKADIY DUBOVOY 0584 Account
Twelve	July 26, 2012	Short trade of approximately 2,000 shares of APKT in the ARKADIY DUBOVOY 6987 Account
Thirteen	April 23, 2013	Short trade of approximately 9,500 shares of EW in the ARKADIY DUBOVOY 6216 Account
Fourteen	April 25, 2013	Purchase of approximately 700 shares of VRSN in the ARKADIY DUBOVOY 6987 Account
Fifteen	October 17, 2013	Purchase of approximately 2,100 shares of ALGN in the ARKADIY DUBOVOY 6987 Account
Sixteen	October 22, 2013	Purchase of approximately 300 shares to cover short sale of PNRA in the ARKADIY DUBOVOY 0584 Account

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

Count Seventeen
(Conspiracy to Commit Fraud and Related Activity in Connection with Computers)

131. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

132. From in or about February 2010 through in or about the present, in the District of New Jersey and elsewhere, defendants

IVAN TURCHYNOV,
a/k/a "Ivan Turchinov,"
a/k/a "Ivan Turchinoff,"
a/k/a "Vladimir Gopienko"
a/k/a "DSU," and
OLEKSANDR IEREMENKO,
a/k/a "Aleksandr Eremenko,"
a/k/a "Zlom,"
a/k/a "Lamarez,"

did knowingly and intentionally conspire and agree with each other and others to, by means of interstate communications, intentionally access protected computers in interstate commerce without authorization, and exceed authorized access, and thereby obtain information from those computers for the purpose of commercial advantage and private financial gain, contrary to Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii).

Object of the Conspiracy

133. It was the object of the conspiracy for defendant TURCHYNOV and defendant IEREMENKO and others to enrich themselves by: (a) gaining unauthorized access to the computer networks of the Victim Newswires, including by misrepresenting their identities in order to gain access to

information that was otherwise off limits to them; (b) stealing confidential business information from those networks, including press releases containing material nonpublic information concerning publicly traded companies – the Stolen Releases; (c) trading ahead of the material nonpublic information contained in the Stolen Releases; and (d) sharing in the proceeds of the profitable illegal trading.

Manner and Means of the Conspiracy

134. It was part of the conspiracy that defendant TURCHYNOV, defendant IEREMENKO and others employed the manner and means set forth in paragraphs 114 through 120 of this Indictment.

Overt Acts

135. In furtherance of the conspiracy and to effect the unlawful objects thereof, defendant TURCHYNOV, defendant IEREMENKO and others committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

a. From in or about July 2010 through in or about January 2011, the Hacker Defendants hacked into the computer networks of PRN.

b. From in or about July 2011 through in or about March 2012, the Hacker Defendants hacked into the computer networks of PRN.

c. On or about March 26, 2012, defendant IEREMENKO sent defendant TURCHYNOV a link to malware placed within the networks of Business Wire.

d. Between on or about March 26, 2012 and on or about June 5, 2012, defendant TURCHYNOV accessed malware that had been installed on Business Wire's networks approximately 39 times.

e. Between on or about April 24, 2012 and on or about July 20, 2012, defendant TURCHYNOV sent SQL Injection Attack commands into the networks of Marketwired on at least 390 occasions.

f. On or about October 10, 2012, defendant IEREMENKO sent an online chat message stating "I'm hacking prnewswire.com."

g. From in or about January 2013 through in or about March 2013, the Hacker Defendants hacked into the computer networks of PRN.

h. On or about July 13, 2015, several Marketwired employees received a phishing email with an attachment that contained a link to malware associated with the 75 IP Address.

In violation of Title 18, United States Code, Section 371.

Counts Eighteen and Nineteen
(Fraud and Related Activity in Connection with Computers)

136. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

137. On or about the dates set forth below, in the District of New Jersey and elsewhere, defendant

IVAN TURCHYNOV,
a/k/a "Ivan Turchinov,"
a/k/a "Ivan Turchinoff,"
a/k/a "Vladimir Gopienko,"
a/k/a "DSU,"

did knowingly and intentionally access protected computers, namely the private, internal networks of PRN, without authorization and in excess of authorized access, and by means of such conduct, did obtain without authorization information from those computers for the purpose of commercial advantage and private financial gain, the value of such information being in excess of $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii), each period of unauthorized access constituting a separate Count of this Indictment:

Count	Approximate Dates of Intrusion
Eighteen	From in or about July 2010 through in or about January 2011
Nineteen	From in or about July 2011 through in or about March 2012

In violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii), and Title 18, United States Code, Section 2.

Count Twenty
(Fraud and Related Activity in Connection with Computers)

138. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

139. From in or about January 2013 through in or about March 2013, in the District of New Jersey and elsewhere, defendants

IVAN TURCHYNOV,
a/k/a "Ivan Turchinov,"
a/k/a "Ivan Turchinoff,"
a/k/a "Vladimir Gopienko"
a/k/a "DSU," and
OLEKSANDR IEREMENKO,
a/k/a "Aleksandr Eremenko,"
a/k/a "Zlom,"
a/k/a "Lamarez,"

did knowingly and intentionally access protected computers, namely the private, internal networks of PRN, without authorization and in excess of authorized access, and by means of such conduct, did obtain without authorization information from those computers for the purpose of commercial advantage and private financial gain, the value of such information being in excess of $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii).

In violation of Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and (c)(2)(B)(iii), and Title 18, United States Code, Section 2.

Count Twenty-One
(Aggravated Identity Theft)

140. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

141. On or about March 28, 2012, in the District of New Jersey and elsewhere, defendant

OLEKSANDR IEREMENKO,
a/k/a "Aleksandr Eremenko,"
a/k/a "Zlom,"
a/k/a "Lamarez,"

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another individual, namely a username and password of Employee #1, during and in relation to a felony violation of a provision enumerated in Title 18, United States Code, Section 1028A(c), that is, conspiracy to commit fraud and related activity in connection with computers as described in Count Seventeen of the Indictment.

In violation of Title 18, United States Code, Section 1028A(a)(1), and Title 18, United States Code, Section 2.

Count Twenty-Two
(Aggravated Identity Theft)

142. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

143. On or about March 28, 2012, in the District of New Jersey and elsewhere, defendant

IVAN TURCHYNOV,
a/k/a "Ivan Turchinov,"
a/k/a "Ivan Turchinoff,"
a/k/a "Vladimir Gopienko"
a/k/a "DSU,"

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another individual, namely a username and password of Employee #2, during and in relation to a felony violation of a provision enumerated in Title 18, United States Code, Section 1028A(c), that is, conspiracy to commit fraud and related activity in connection with computers as described in Count Seventeen of the Indictment.

In violation of Title 18, United States Code, Section 1028A(a)(1), and Title 18, United States Code, Section 2.

Count Twenty-Three
(Money Laundering Conspiracy)

144. The allegations contained in paragraphs 1 through 110 of this Indictment are realleged and incorporated as though fully set forth in this paragraph.

145. From in or about February 2010 through in or about the present, in Bergen, Hudson, and Middlesex Counties, in the District of New Jersey and elsewhere, defendants

IVAN TURCHYNOV,
a/k/a "Ivan Turchinov,"
a/k/a "Ivan Turchinoff,"
a/k/a "Vladimir Gopienko"
a/k/a "DSU,"
OLEKSANDR IEREMENKO,
a/k/a "Aleksandr Eremenko,"
a/k/a "Zlom,"
a/k/a "Lamarez,"
ARKADIY DUBOVOY,
IGOR DUBOVOY, and
PAVEL DUBOVOY

did knowingly combine, conspire, and agree with each other and others to commit offenses against the United States in violation of Title 18, United States Code, Sections 1956 and 1957, to wit:

a. to knowingly conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of specified unlawful activity, that is, the wire fraud, securities fraud, computer-related fraud, and conspiracy offenses alleged in Counts One through Twenty of this Indictment, with the intent to promote the carrying on of such specified unlawful activity, and that while conducting and attempting

to conduct such financial transactions knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity in violation of Title 18, United States Code, Section 1956(a)(1)(A)(i);

b. to knowingly conduct and attempt to conduct financial transactions affecting interstate commerce and foreign commerce, which transactions involved the proceeds of specified unlawful activity, that is, the wire fraud, securities fraud, computer-related fraud, and conspiracy offenses alleged in Counts One through Twenty of this Indictment, knowing that the transactions were designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, and that while conducting and attempting to conduct such financial transactions, knew that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i);

c. to knowingly transport, transmit, and transfer monetary instruments and funds from a place in the United States to a place outside the United States, by wire and other means, with the intent to promote the carrying on of specified unlawful activity, that is, the wire fraud, securities fraud, computer-related fraud, and conspiracy offenses alleged in Counts One through Twenty of this Indictment, contrary to Title 18, United States Code, Section 1956(a)(2)(A);

d. to transport, transmit, and transfer, and attempt to transport, transmit, and transfer a monetary instrument or funds involving the

proceeds of specified unlawful activity, that is, the wire fraud, securities fraud, computer-related fraud, and conspiracy offenses alleged in Counts One through Twenty of this Indictment, from a place in the United States to or through a place outside the United States, by wire and other means, knowing that the funds involved in the transportation, transmission, and transfer represented the proceeds of some form of unlawful activity and knowing that such transportation, transmission, and transfer was designed in whole or in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity, in violation of Title 18, United States Code, Section 1956(a)(2)(B)(i); and

e. to knowingly engage and attempt to engage, in monetary transactions by, through, or to a financial institution, in and affecting interstate and foreign commerce, in criminally derived property of a value greater than $10,000, that is, the deposit, withdrawal, transfer, and exchange of United States currency, funds, and monetary instruments by wire and other means, such property having been derived from specified unlawful activity, namely, the wire fraud, securities fraud, computer-related fraud, and conspiracy offenses alleged in Counts One through Twenty of this Indictment, in violation of Title 18, United States Code, Section 1957.

In violation of Title 18, United States Code, Section 1956(h).

FORFEITURE ALLEGATION AS TO COUNTS ONE THROUGH SIXTEEN

As a result of committing the offenses constituting specified unlawful activity, as defined in 18 U.S.C. § 1956(c)(7), as charged in Counts One through Sixteen of this Indictment, the defendants charged in each respective count shall forfeit to the United States, pursuant to 18 U.S.C. § 981(a)(1)(C) and 28 U.S.C. § 2461(c), all property, real and personal, that constitutes or is derived from proceeds traceable to the commission of the offense charged in each such count, and all property traceable to such property, including but not limited to all right, title, and interest of the defendants in the following:

(a) Interactive Brokers account number ending in 1184 held in the name of M&I Advising Associates LLC;

(b) TradeKing Securities account number ending in 8312 held in the name of Arkadiy Dubovoy;

(c) Scottrade, Inc. account number ending in 0584 held in the name of Arkadiy Dubovoy;

(d) Interactive Brokers account number ending in 7635 held in the name of Boni, Inc.;

(e) MB Trading, Inc. account number ending in 1787 held in the name of Arkadiy Dubovoy;

(f) Options House LLC Account Number ending in 0944 held in the name of Boni, Inc.;

(g) Etrade Securities Account Number ending in 6987 held in the name of Arkadiy Dubovoy;

(h) Fidelity Investments Account Number ending in 6216 held in the name of Arkadiy Dubovoy;

(i) ETrade Securities Account Number ending in 7579 held in the name of Southeastern Holdings and Investment, LLC;

(j) All rights, title, and interest, including all appurtenances and improvements thereon, in the property located at 6390 Putnam Ford Road, Woodstock, Georgia 30189; and

(k) One 1999 Sumerset Houseboat, Hull ID SZJ02656I899;

and all property traceable to such property, (hereinafter referred to collectively as the "Specific Properties").

FORFEITURE ALLEGATION AS TO COUNTS SEVENTEEN THROUGH TWENTY

146. As a result of committing the offenses alleged in Counts Seventeen through Twenty of this Indictment, the defendants charged in each respective count shall forfeit to the United States.

a. pursuant to 18 U.S.C. §§ 982(a)(2)(B) and 1030(i), any property, real or personal, constituting, or derived from, proceeds obtained directly or indirectly as a result of the offense charged in each such count; and

b. pursuant to 18 U.S.C. § 1030(i), any personal property that was used or intended to be used to commit or to facilitate the commission of the offense charged in each such count.

FORFEITURE ALLEGATION AS TO COUNT TWENTY-THREE

147. As a result of committing the money laundering conspiracy offense in violation of 18 U.S.C. § 1956(h) alleged in Count Twenty-Three of this Indictment, defendants charged in that count shall forfeit to the United States, pursuant to 18 U.S.C. § 982(a)(1), all property, real and personal, involved in such money laundering conspiracy offense, and all property traceable to such

property, including but not limited to all right, title, and interest of the defendants in the Specific Properties.

SUBSTITUTE ASSETS PROVISION
(Applicable to All Forfeiture Allegations)

148. If any of the above-described forfeitable property, as a result of any act or omission of a defendants:

a. cannot be located upon the exercise of due diligence;

b. has been transferred or sold to, or deposited with a third party;

c. has been placed beyond the jurisdiction of the court;

d. has been substantially diminished in value; or

e. has been commingled with other property which cannot be divided without difficulty;

the United States shall be entitled, pursuant to 21 U.S.C. § 853(p) (as incorporated by 28 U.S.C. § 2461(c), 18 U.S.C. § 1030(i), and 18 U.S.C. § 982(b)), to forfeiture of any other property of the defendants up to the value of the above-described forfeitable property.

A TRUE BILL,

[redacted]

Grand Jury Foreperson

PAUL J. FISHMAN
United States Attorney