UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
	:	**SEALED SUPERSEDING**
-v.-	:	**INDICTMENT**
	:	
ANDREI TYURIN, a/k/a "Andrei Tiurin,"	:	S3 15 Cr. 333 (LTS)
	:	
Defendant.	:	

COUNT ONE
(Conspiracy to Commit Computer Hacking)

The Grand Jury charges:

Relevant Persons and Entities

1. At all times relevant to this Indictment, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, was a citizen and resident of Russia. At all relevant times, TYURIN conspired with an individual not named as a defendant herein ("CC-1"), among others, to engage in a series of computer hacking crimes, in furtherance of CC-1's sprawling cybercriminal enterprise.

2. At all relevant times, Victim-1 was one of the world's largest financial institutions, with headquarters in New York, New York.

3. At all relevant times, Victim-2 was one of the world's largest financial services corporations, providing mutual fund,

online stock brokerage and other services, with headquarters in Boston, Massachusetts.

4. At all relevant times, Victim-3 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in Omaha, Nebraska.

5. At all relevant times, Victim-4 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in New York, New York.

6. At all relevant times, Victim-5 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in St. Louis, Missouri.

7. At all relevant times, Victim-6 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in Queens, New York.

8. At all relevant times, Victim-7 was a U.S.-based financial services corporation, providing online stock brokerage and other services, with headquarters in Charlotte, North Carolina.

9. At all relevant times, Victim-8 was one of the world's most widely circulated financial news publications, with headquarters in New York, New York.

10. At all relevant times, Victim-9 was a financial news publisher, with headquarters in Baltimore, Maryland.

11. At all relevant times, Victim-10 was a software development firm, with headquarters in Costa Rica and offices in the United States.

12. At all relevant times, Victim-11 was a software development firm, with headquarters in Curaçao.

13. At all relevant times, Victim-12 was a merchant risk intelligence firm, with headquarters in Bellevue, Washington.

Overview

14. From approximately 2012 to mid-2015, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, conducted massive computer hacking crimes against U.S. financial institutions, financial services corporations, and financial news publishers, including the largest theft of customer data from a U.S. financial institution in history (the "U.S. Financial Sector Hacks"). TYURIN conducted these network intrusions, which included the intrusions into Victims 1 through 9, among others, at the direction of CC-1. These intrusions resulted in the theft of the personal information of over one hundred million customers of these victim companies. TYURIN, CC-1, and their co-conspirators engaged in these crimes in furtherance of other criminal schemes that were overseen by CC-1, including securities market manipulation schemes perpetrated in the United States. In particular, in an effort to artificially manipulate

the price of certain stocks publicly traded in the United States, CC-1 and other co-conspirators sought to market the stocks, in a deceptive and misleading manner, to customers of the victim companies whose contact information TYURIN had accessed and stolen in the intrusions. CC-1 and these co-conspirators generated tens of millions of dollars in unlawful proceeds from these schemes in part due to TYURIN's efforts.

15. In addition to conducting the U.S. Financial Sector Hacks, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, conducted computer network hacks and cyberattacks against numerous United States and foreign companies outside of the financial sector. As set forth below, TYURIN, CC-1, and their co-conspirators engaged in these crimes in furtherance of large-scale criminal businesses that CC-1 operated in the United States and other countries. In particular, between approximately 2007 and July 2015, CC-1 owned and operated unlawful internet gambling businesses in the United States and abroad; and owned and operated multinational payment processors for illegal pharmaceutical suppliers, counterfeit and malicious software ("malware") distributors, and unlawful internet casinos. Nearly all of these schemes, like TYURIN and CC-1's securities market manipulation schemes, relied for their success on computer hacking and other cybercrimes committed by TYURIN at

CC-1's request. Through these criminal schemes, between in or about 2007 and in or about July 2015, TYURIN, CC-1, and their co-conspirators earned hundreds of millions of dollars in illicit proceeds.

Execution of the U.S. Financial Sector Hacks

16. ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, CC-1, and their co-conspirators executed the U.S. Financial Sector Hacks using the following means and methods:

a. In furtherance of the conspiracy, using aliases, CC-1 and, at CC-1's direction, certain co-conspirators not identified herein, procured computer network infrastructure, including particular servers located in Egypt, the Czech Republic, South Africa, Brazil, Turkey, and elsewhere, to be used by TYURIN to gain unlawful access to companies' computer networks and to receive data stolen from those networks during the intrusions.

b. Also in furtherance of the conspiracy, at various times, CC-1 directed TYURIN to execute network intrusions at particular companies in an effort to steal customer data as identified by CC-1, in conjunction with another co-conspirator not named as a defendant herein ("CC-2").

c. As a further part of the conspiracy, in connection with many of the network intrusions, CC-2 provided to

CC-1, CC-2's own login credentials and other information obtained by CC-2, as a customer of many of the victim companies. CC-1 in turn provided this information to TYURIN, who used that information to perform certain analyses of those victims' networks in connection with the intrusions.

d. Also in furtherance of the conspiracy, at CC-1's direction, TYURIN hacked into the victims' network servers, on which TYURIN typically caused a particular piece of malware to be installed. This malware provided TYURIN with persistent access to many of the victim companies' networks, enabling TYURIN and CC-1 to steal data from these victims repeatedly, sometimes over a period of many months.

e. As a further part of the conspiracy, as TYURIN and CC-1 engaged in particular network intrusions at CC-1's direction, TYURIN and CC-1 discussed the nature of the data TYURIN was locating and stealing at CC-1's direction, various issues TYURIN encountered while hacking into the networks, and CC-1's receipt and use of the stolen data.

f. Also in furtherance of the conspiracy, after obtaining stolen customer data from victim companies, CC-1, CC-2, and their co-conspirators used or sought to use the data in furtherance of their other criminal schemes, including various

securities market manipulation schemes directed at U.S. financial markets.

The 2012-2013 Hacks

17. Between approximately 2012 and late 2013, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, working with CC-1 and CC-2, executed the hacks of the computer networks of Victims 4 through 9, stealing records relating to tens of millions of customers of these institutions. Among other things, in electronic communications during these hacks:

a. CC-1 bragged about the size and scope of his securities market manipulation schemes, and described to TYURIN his use of the stolen data in furtherance of those schemes. For example:

i. As to a particular publicly traded stock for which CC-1, CC-2, and their co-conspirators had manipulated trading in the United States, CC-1 boasted that his sale of that stock for large profits was "a small step towards a large empire." As CC-1 explained, "We buy them [i.e., stocks] very cheap, perform machinations, then play with them. . ." When TYURIN asked, with respect to CC-1's ability to cause people in the United States to purchase stocks, if it really was "popular in America - buying stocks?," CC-1 responded, "It's like drinking freaking vodka in Russia."

ii. CC-1 indicated to TYURIN that CC-1 intended to distribute "mailers," or promotions of particular stocks, to people whose contact information TYURIN had stolen from the victim companies.

iii. CC-1 described to TYURIN contacting and lying to people whose personal information had been obtained in the hacks, in the course of tricking those people into buying stocks being deceptively touted by the defendants. In particular, CC-1 explained, individuals acting at CC-1's direction lied to people about how their personal contact information had been obtained, falsely claiming that the information was simply "in our investors' database."

b. TYURIN and CC-1 discussed expanding the size and scope of their network intrusions to encompass thefts of material non-public information from the financial institutions and other firms they were hacking. For example, TYURIN noted, "the top managers in [Victim-5], can they have some interesting info in their mail [i.e., email]? Regarding working on the stock market, etc. It's a big company after all. mb [Maybe] they have some secrets. . . What do you think?" CC-1 responded, "Yes, this is a very cool idea. Some *inside* [i.e., inside, or material non-public, information]. We need to think how we can do it."

The 2014 Hacks

18. In 2014, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, CC-1, and their co-conspirators orchestrated network intrusions into even bigger financial institutions, including Victims 1 through 3. In particular, in or about March 2014, TYURIN, CC-1, and their co-conspirators began their efforts to hack into the computer networks of Victim-3. As part of that effort, they repeatedly attempted to access CC-2's Victim-3 customer account from a particular Egypt-based computer server (the "Egypt Server"), but they were unable to do so because, after observing the attempts to access the account from this server, Victim-3 locked CC-2's account for online access. In response, and in furtherance of the hack, CC-2 called Victim-3 and, upon being notified that his account had been locked and asked by a customer service representative whether CC-2 had been traveling in Egypt in March 2014, CC-2 lied to the representative, and claimed that he had been in Egypt. In truth and in fact, and as CC-2 well knew, CC-2 had not been in Egypt, and was merely attempting to convince Victim-3 to allow CC-2 and his co-conspirators to access CC-2's account online in furtherance of their efforts to hack into Victim-3.

19. Thereafter, in April 2014, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, CC-1, and their co-conspirators

unlawfully accessed the network of Victim-2 by exploiting the so-called "Heartbleed" vulnerability, which had, at that time, just been widely identified as a previously unrecognized security vulnerability that existed in computer network servers on a widespread basis. While they succeeded in gaining access to Victim-2's network, shortly after they did so, Victim-2 recognized and repaired the Heartbleed vulnerability in its systems. In foreign-language electronic communications dated April 2014, TYURIN told CC-1, in substance and in part, that he no longer had access to Victim-2's networks, because, as a result of reports of the vulnerability in the news, "[Victim-2] started fixing it" within their systems, thus leaving TYURIN without access.

20. In foreign-language electronic communications dated May 2014, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, provided to CC-1 the login information for a customer of Victim-3, which CC-1 used to log into the customer's account, and then remarked to TYURIN "[Expletive], he has 202K Balance . . . . worth of stock" and "$145" thousand in cash "to take . . . out" of the account. TYURIN and CC-1 then discussed various ways they could exploit this type of account access, including potentially trading stocks or withdrawing funds, which possibilities CC-1 described as "simply [expletive] awesome."

TYURIN warned CC-1 not to do anything, because "if two, three people complain, [Victim-3] will start [a] serious investigation, [t]hey will check logins and change all passwords." Instead, TYURIN noted that they should do "[n]othing so far, I think. We will think about it."

21. Beginning in June 2014, and ending in August 2014, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, CC-1, CC-2, and their co-conspirators executed the hack of Victim-1, during which they stole customer records of over 83 million customers of Victim-1.

a. As included in foreign-language electronic communications dated June 2014, CC-1 identified Victim-1 as an investment institution "[w]e need to break into" because Victim-1 had "asset managers, the biggest ones." CC-1 specifically noted that Victim-1 was important because "[a]ll of America is there" in Victim-1's databases.

b. To hack into Victim-1's network, TYURIN, CC-1, and their co-conspirators used, among others, the Egypt Server, which they had rented from a third-party company for years under an alias frequently used by CC-1, CC-2, and their co-conspirators in the course of their criminal schemes. In furtherance of their efforts to hack Victim-1, TYURIN also asked CC-1 to register a domain name for the intrusion. CC-1

subsequently registered a domain name that included Victim-1's name, which enabled TYURIN, CC-1, and their co-conspirators to reroute internet traffic that was intended for Victim-1 to go instead to a server under TYURIN and CC-1's control. CC-1 also provided to TYURIN the login information for CC-2. Later that day, TYURIN told CC-1 that he had almost gained access to one of Victim-1's servers.

c. On or about July 4, 2014, TYURIN noted to CC-1 that he was "inside [Victim-1's] network," to which CC-1 responded "Wow, very cool." TYURIN noted "Yes, I can say that half the work is done." TYURIN later asked CC-1 "[w]ill there be a lot of benefit from" access to Victim-1's customer data, to which CC-1 responded "[expletive] loads!"

d. On or about July 25, 2014, TYURIN wrote to CC-1 that he had "found some databases" within Victim-1's systems, and that there were "a lot of databases . . . and even more servers," noting that traversing Victim-1's network infrastructure in search of its customer database was like "opening a book in the middle . . . to look for a sentence not knowing where exactly" to start. CC-1 responded "Very good." Three days later, TYURIN found CC-2's account information within Victim-1's systems, along with the information of "85 million" customers "in the database." The next day, CC-1 stated, in

response, that "[Victim-1] is just simply the [expletive]." TYURIN responded that he had "downloaded a few million addresses" of Victim-1's customers already from Victim-1's servers.

e. On or about August 1, 2014, TYURIN wrote to CC-1 that he had downloaded "90% of [Victim-1's] information," and noted that he had completed the download about four days thereafter. On or about August 16, 2014, TYURIN stated to CC-1 that it appeared that their intrusion into Victim-1's systems "was detected" because a few of the Internet Protocol ("IP") addresses that TYURIN had been using in his intrusion of Victim-1 had been "banned" from the systems. CC-1 responded that if the IPs had been banned then they "probably were caught."

f. Later that month, on or about August 28, 2014, CC-1 sent to TYURIN a link to a foreign-language news article reporting on Victim-1's hack, and asked TYURIN, "Did you see this [expletive?] I think we need to kill the servers." TYURIN responded that he agreed, and provided the IP addresses of four servers that were used in furtherance of the hack of Victim-1, including the Egypt Server. TYURIN sent to CC-1 a link to an English language news article also reporting about the hack, and stated "We're caught . . . I wasn't careful doing something," to which CC-1 responded "[Expletive] it. Forget it, we are killing

the servers." Shortly thereafter, the rental of the Egypt Server was cancelled.

The Securities Market Manipulation Schemes

22. From in or about 2011 up to and including July 2015, TYURIN, CC-1, CC-2, and their co-conspirators engaged in lucrative securities market manipulation schemes in the United States. In order to facilitate these schemes, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, conducted a series of computer hacks to steal customer data from Victims 1 through 9, so that CC-1, CC-2, and other co-conspirators could send various deceptive marketing materials involving particular targeted stocks to U.S.-based customers of Victims 1 through 9. In furtherance of their securities market manipulation scheme, among other things:

a. CC-1 and CC-2 identified opportunities to partner with "promoters," who identified companies whose stock would be targeted for manipulation. Upon partnering with the promoters, CC-1, CC-2, and the promoters agreed upon the compensation that CC-1 and CC-2 would receive for their role in the scheme, which was typically either hundreds of thousands of dollars, or shares in the targeted stock that the co-conspirators often sold for up to millions of dollars in profits per stock in the course of the scheme.

b. Also in furtherance of the securities fraud scheme, the promoters - along with, at certain times, CC-1 and CC-2 - acquired control over all or substantially all of the free-trading shares of the targeted stock, that is, shares that the owner could trade without restriction on a national stock exchange or in the over-the-counter market. At certain times, when they acquired such shares, CC-1 and CC-2 held the shares in particular U.S. brokerage accounts, which were frequently held in the names of shell companies controlled by the co-conspirators using numerous aliases, false passports and other false personal identification information.

c. As a further part of the securities fraud scheme, after members of the conspiracy acquired control of a substantial portion of the free-trading shares of the targeted stock, CC-1 and CC-2, with the aid of various of their co-conspirators, artificially inflated the stock's price and trading volume through two primary fraudulent and deceptive means. First, certain members of the conspiracy typically executed pre-arranged manipulative trades to cause the stock's price to rise small amounts on successive days. Second, in connection with that trading, CC-1 and CC-2 began disseminating materially misleading, unsolicited ("spam") messages by various means - including by email to up to millions of recipients per

day - that falsely touted the stock in order to trick others into buying it. TYURIN, along with CC-1, engaged in the U.S. Financial Sector Hacks in part to acquire email and mailing addresses, phone numbers and other contact information of potential victims to whom they could send such deceptive communications. As orchestrated by the co-conspirators, these communications contained materially false and fraudulent statements including, for example: (i) that the stock's recent trading activity reflected legitimate demand for the stock (when in truth and in fact, and as the co-conspirators well knew, the trading activity was caused in whole or part by their co-conspirators' manipulative trading); and (ii) that the emails were being distributed and financed by certain third parties (when, in truth and in fact, and as the co-conspirators well knew, the emails were being distributed and financed by CC-1, CC-2 and their co-conspirators, who controlled all or nearly all of the free-trading shares of the stock, using customer data that TYURIN had stolen in furtherance of the scheme). In addition to fraudulently promoting the stocks by email, CC-1 and CC-2 fraudulently marketed the stocks to potential U.S. victims by mail and phone, again using data that TYURIN had stolen.

d. Also in furtherance of the conspiracy, after causing the stock's price and trading volume to increase

artificially during the days or weeks of the deceptive promotional campaign, members of the conspiracy began selling their shares in a coordinated fashion, often resulting in millions of dollars in profits per stock to members of the conspiracy. The co-conspirators' massive coordinated sales typically placed downward pressure on the stock's price and caused its trading volume to plummet, exposing unsuspecting investors to significant losses. CC-1, CC-2, and their co-conspirators earned millions of dollars in illicit profits this way. For example, among the dozens of publicly traded stocks for which they successfully manipulated trading, CC-1, CC-2, and their co-conspirators sold their holdings in a particular stock ("Stock-1") for over $2 million at artificially inflated prices, soon after which Stock-1's price and liquidity plummeted.

The Unlawful Internet Gambling Schemes, Hacks and Cyberattacks

23. In addition to committing the U.S. Financial Sector Hacks in furtherance of U.S. securities market manipulation schemes, from at least in or about 2012 up to and including in or about July 2015, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, CC-1, and their co-conspirators engaged in massive hacks and cyberattacks in furtherance of CC-1's operation of lucrative, unlawful internet casinos in the United States and elsewhere, which CC-1 ran with the assistance of hundreds of

employees in multiple countries. TYURIN, CC-1, and their co-conspirators engaged in these hacks and cyberattacks against other internet gambling businesses to steal customer information, secretly review executives' emails, and cripple rival businesses. In particular, in or about 2012, CC-1, with the assistance of TYURIN and others, orchestrated network intrusions of competitors in order to steal CC-1's competitors' customer databases and other information. CC-1 separately directed "distributed denial of service," or DDOS, attacks, against competitors to temporarily shut down their businesses in response to perceived misconduct by them directed at CC-1's casinos.

24. Also in furtherance of CC-1's unlawful internet gambling businesses, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, at CC-1's request, executed network intrusions of Victim-10 and Victim-11, software development companies that provided operating software to CC-1's internet casinos and other such casinos around the world. In doing so, CC-1 sought to, and did, secretly obtain access to the email accounts of senior executives at both companies, reading their emails on an ongoing basis, a fact CC-1 ultimately admitted to at least one of the executives whose emails he had been secretly reading. CC-1, with the assistance of TYURIN, monitored company executives'

emails in order to ensure that the companies' work with CC-1's competitors did not, in CC-1's view, compromise the success of CC-1's unlawful internet gambling businesses.

The Illicit Payment Processing Scheme and Hack

25. From at least in or about 2012 up to and including in or about July 2015, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, CC-1, and their co-conspirators also engaged in cyber intrusion activity in furtherance of CC-1's operation of multinational payment processors for criminals who sought to receive payments by credit and debit card in furtherance of their unlawful schemes. Through these payment processors, CC-1 and other co-conspirators knowingly processed credit and debit card payments for, at a minimum, unlawful pharmaceutical distributors, purveyors of counterfeit and malicious purported "anti-virus" computer software, their own unlawful internet casinos, and an illegal United States-based Bitcoin exchange owned by CC-1. In doing so, CC-1 and other co-conspirators knowingly processed hundreds of millions of dollars in transactions for criminal schemes, for which they earned a percentage of every transaction, amounting to over $18 million in illicit profits.

26. As CC-1 and these co-conspirators well knew, banks and credit card issuers in the United States and elsewhere were

largely unwilling to process payment transactions for illegal activities such as internet gambling, the sale of counterfeit pharmaceuticals, the distribution of counterfeit and malicious software, and running an unlicensed Bitcoin exchange. For that reason, to open and operate bank accounts in numerous countries, including Azerbaijan, through which they processed unlawful credit and debit card transactions, CC-1 and these co-conspirators variously lied to financial institutions about the nature of their business and colluded with corrupt international bank officials who willfully ignored its criminal nature in order to profit from, as a co-conspirator described it to CC-1, their payment processing "casino/soft[ware]/pharma[ceutical] cocktail." Furthermore, to deceive U.S. banks and credit card issuers into authorizing their illicit credit and debit card payment transactions, CC-1 and these co-conspirators deliberately misidentified and miscoded those transactions, in violation of bank and credit card company rules and regulations.

27. At relevant times, in an effort to ensure compliance with their regulations, major United States credit card companies monitored and investigated merchant activity that appeared to be in furtherance of criminal schemes or otherwise designed to circumvent their regulations. In the course of that work, credit card companies repeatedly identified bank accounts

which were receiving credit and debit card payments for illicit pharmaceuticals and other criminal goods and services, and which, unbeknownst to the credit card companies, were operated by CC-1 and other co-conspirators in furtherance of their unlawful payment processing scheme. In so doing, the credit card companies imposed millions of dollars in penalties on the financial institutions through which CC-1 and other co-conspirators processed these unlawful credit and debit card payments, in certain cases shutting down the processing of certain bank accounts. CC-1 and other co-conspirators, in turn, paid those amounts to the financial institutions to cover the penalties.

28. Beginning in or about 2012, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, CC-1, and their co-conspirators hacked into the computer networks of Victim-12, a U.S. company which assessed merchant risk and compliance for credit card issuers and others, including by detecting merchants that accepted credit card payments for unlawful goods or services. TYURIN, CC-1, and their co-conspirators did so in an effort to avoid further financial penalties and processing shutdowns, and to evade law enforcement detection of their illicit payment processing scheme. Thereafter, on an ongoing basis, TYURIN, CC-1, and their co-conspirators monitored Victim-12's detection

efforts, including reading emails of Victim-12 employees, so they could take steps to evade detection by Victim-12 of their unlawful payment processing scheme. In particular, through their unlawful intrusion into Victim-12's network, TYURIN, CC-1, and their co-conspirators determined which credit and debit card numbers Victim-12 employees were using to make undercover purchases of illicit goods in the course of their effort to detect unlawful merchants. Upon identifying those credit and debit card numbers, CC-1 and other co-conspirators blacklisted the numbers from their payment processing business, automatically declining any transaction for which payment was offered through one of those credit or debit card numbers.

Statutory Allegations

29. From at least in or about 2012, up to and including at least July 2015, in the Southern District of New York and elsewhere, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit an offense against the United States, to wit, computer hacking, in violation of Title 18, United States Code, Sections 1030(a)(2)(A), 1030(a)(2)(C), 1030(a)(4), and 1030(c).

30. It was a part and an object of the conspiracy that ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others

known and unknown, would and did intentionally access a computer without authorization and exceed authorized access, and thereby obtain information contained in a financial record of a financial institution, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal act in violation of the laws of the United States, to wit, securities fraud, in violation of Title 15, United States Code, Sections 78j(b) & 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5, the value of which information exceeded $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(A) and 1030(c)(2)(B).

31. It was a further part and an object of the conspiracy that ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, would and did intentionally access a computer without authorization and exceed authorized access, and thereby obtain information from a protected computer, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal act in violation of the laws of the United States, to wit, securities fraud, in violation of Title 15, United States Code, Sections 78j(b) & 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5, the value of which information exceeded $5,000, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B).

32. It was a further part and an object of the conspiracy that ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, would and did knowingly and with intent to defraud, access a protected computer without authorization, and exceed authorized access, and by means of such conduct further the intended fraud and obtain a thing of value, to wit, customer information and data that was used in furtherance of securities fraud crimes, the value of which information exceeded $5,000 in a 1-year period, in violation of Title 18, United States Code, Section 1030(a)(4) and 1030(c)(3)(A).

Overt Acts

33. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. In or about June 2012, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, caused the unauthorized access to, and theft of customer data from, the computer network of Victim-9.

b. In or about December 2012, TYURIN caused the unauthorized access to, and theft of customer data from, Victim-

6, including by wire communications through the Southern District of New York.

c. In or about August 2013, TYURIN caused the unauthorized access to, and theft of customer data from, the computer network of Victim-8.

d. On or about August 30, 2013, while hacking into Victim-8's computer network, TYURIN told CC-1, in electronic communications, in substance, that TYURIN had located 10 million email addresses of Victim-8 customers.

e. During at least in or about September 2013 to in or about February 2014, TYURIN caused the unauthorized access to, and theft of customer data from, the computer network of Victim-5.

f. During at least in or about September 2013 to in or about November 2013, TYURIN caused the unauthorized access to, and theft of customer data from, the computer network of Victim-7.

g. In or about December 2013, TYURIN caused the unauthorized access to, and theft of customer data from, the computer network of Victim-4.

h. On or about December 7, 2013, while hacking into Victim-4's computer network, TYURIN told CC-1, in electronic

communications, in substance, that TYURIN had located 15 million email addresses of Victim-4 customers.

i. In or about April 2014, TYURIN caused Victim-2's computer network to be accessed without authorization.

j. From in or about June 2014, to in or about August 2014, TYURIN caused the unauthorized access to, and theft of customer data from, the computer network of Victim-1.

k. In or about August 2014, upon the publication of news stories relating to the hacking of Victim-1, TYURIN directed CC-1 to cancel a subscription to servers that were used to access Victim-1's computer network without authorization.

(Title 18, United States Code, Section 371.)

COUNT TWO
(Wire Fraud)

The Grand Jury further charges:

34. The allegations contained in paragraphs 1 through 28 and 33 of this Indictment are repeated and realleged as if fully set forth herein.

35. From at least in or about 2012, up to and including at least July 2015, in the Southern District of New York and elsewhere, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would

and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, and did aid and abet the same, to wit, TYURIN accessed without authorization the networks of various companies for the purpose of exfiltrating customer information and data that was used in furtherance of securities fraud crimes.

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

COUNT THREE

(Computer Hacking: Victim-1)

The Grand Jury further charges:

36. The allegations contained in paragraphs 1 through 28 and 33 of this Indictment are repeated and realleged as if fully set forth herein.

37. From at least in or about June 2014, up to and including at least in or about August 2014, in the Southern District of New York and elsewhere, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, intentionally accessed a computer without authorization and exceeded authorized access, and thereby obtained information contained in a financial record of a financial institution and from a protected computer, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal act in violation of the laws of the

United States, to wit, securities fraud, in violation of Title 15, United States Code, Sections 78j(b) & 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5, the value of which information exceeded $5,000, to wit, TYURIN hacked into the computer network of Victim-1 to steal personal information of tens of millions of Victim-1 customers in furtherance of securities fraud schemes perpetrated by his co-conspirators.

(Title 18, United States Code, Sections 1030(a)(2)(A), 1030(a)(2)(C), 1030(c)(2)(B), and 2.)

COUNT FOUR
(Computer Hacking: Victim-1)

The Grand Jury further charges:

38. The allegations contained in paragraphs 1 through 28 and 33 of this Indictment are repeated and realleged as if fully set forth herein.

39. From at least in or about June 2014, up to and including at least in or about August 2014, in the Southern District of New York and elsewhere, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, knowingly and with intent to defraud, accessed a protected computer without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained a thing of value which exceeded $5,000 in a 1-year period, to wit, TYURIN hacked into the computer network of Victim-1 to steal personal information

of tens of millions of Victim-1 customers in furtherance of securities fraud schemes perpetrated by TYURIN and his co-conspirators.

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

COUNT FIVE
(Computer Hacking: Victim-8)

The Grand Jury further charges:

40. The allegations contained in paragraphs 1 through 28 and 33 of this Indictment are repeated and realleged as if fully set forth herein.

41. From at least in or about late 2013, up to and including in or about May 2015, in the Southern District of New York and elsewhere, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, intentionally accessed a computer without authorization and exceeded authorized access, and thereby obtained information from a protected computer, for purposes of commercial advantage and private financial gain, and in furtherance of a criminal act in violation of the laws of the United States, to wit, securities fraud, in violation of Title 15, United States Code, Sections 78j(b) & 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5, the value of which information obtained exceeded $5,000, to wit, TYURIN hacked into the computer network of Victim-8 to steal personal

information of millions of Victim-8 customers in furtherance of securities fraud schemes perpetrated by TYURIN and his co-conspirators.

(Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B), and 2.)

COUNT SIX

(Computer Hacking: Victim-8)

The Grand Jury further charges:

42. The allegations contained in paragraphs 1 through 28 and 33 of this Indictment are repeated and realleged as if fully set forth herein.

43. From at least in or about late 2013, up to and including in or about May 2015, in the Southern District of New York and elsewhere, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, knowingly and with intent to defraud, accessed a protected computer without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained a thing of value which exceeded $5,000 in a 1-year period, to wit, TYURIN hacked into the computer network of Victim-8 to steal personal information of millions of Victim-8 customers in furtherance of fraud schemes perpetrated by TYURIN and his co-conspirators.

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

COUNT SEVEN

(Conspiracy to Commit Securities Fraud)

The Grand Jury further charges:

44. The allegations contained in paragraphs 1 through 28 and 33 of this Indictment are repeated and realleged as if fully set forth herein.

45. From at least in or about 2011, up to and including in or about July 2015, in the Southern District of New York and elsewhere, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated and agreed together and with each other to commit an offense against the United States, to wit, securities fraud, in violation of Title 15, United States Code, Section 78j(b) and 78ff, and Title 17, Code of Federal Regulations, Section 240.10b-5.

46. It was a part and an object of the conspiracy that ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, willfully and knowingly, directly and indirectly, by use of the means and instrumentalities of interstate commerce, and of the mails, and of the 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 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 any person, in violation of Title 15, United States Code, Sections 78j(b) and 78ff.

Overt Acts

47. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about June 12, 2011, by email from outside the United States to a securities brokerage firm located in New York, New York ("Firm-1"), a co-conspirator not named as a defendant herein ("CC-3") opened an account at Firm-1 in the name "Entersa Limited" using an alias and a false passport (the "Firm-1 Entersa Account").

b. In or about June 2011, by email and telephone, CC-2 informed a representative of Firm-1 in New York, New York that email promotional campaigns run by CC-1, CC-2, and others

had resulted in substantial trading volume in ten particular publicly traded stocks on particular dates.

c. In or about early January 2012, CC-2 transferred 2.5 million shares of Stock-1 into the Firm-1 Entersa Account in New York, New York.

d. In or about late January 2012, CC-1 and CC-2 caused spam emails touting Stock-1, including false statements about the cause of the increase in Stock-1's trading volume, to be widely disseminated to recipients throughout the United States.

e. From on or about January 30, 2012 to on or about February 13, 2012, Entersa's Stock-1 holdings at Firm-1, located in New York, New York, were liquidated and, at the direction of CC-2, Firm-1 wired over $1.1 million in proceeds to a bank account in Cyprus in the name of Entersa ("the Entersa Cyprus Account").

f. In or about September 2013, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and CC-1 discussed a stock manipulation scheme that would require use of the "exchange" in "New York, [in] America."

(Title 18, United States Code, Section 371.)

COUNT EIGHT

(Unlawful Internet Gambling Enforcement Act Conspiracy)

The Grand Jury further charges:

48. The allegations contained in paragraphs 1 through 28, 33 and 47 of this Indictment are repeated and realleged as if fully set forth herein.

49. From at least in or about 2007, up to and including in or about July 2015, in the Southern District of New York and elsewhere, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit offenses against the United States, to wit, violations of Title 31, United States Code, Section 5363.

50. It was a part and an object of the conspiracy that ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, willfully and knowingly, while engaged in the business of betting and wagering, would and did knowingly accept, in connection with the participation of another person in unlawful internet gambling, to wit, gambling in violation of New York Penal Law Sections 225.00 and 225.05 and the laws of other states where the gambling businesses operated, credit, and the proceeds of credit, extended to and on behalf of such other person, including credit extended through the use of a credit card, and an electronic fund transfer and the proceeds of an

electronic fund transfer from and on behalf of such other person, and a check, draft and similar instrument which is drawn by and on behalf of such other person and is drawn on and payable at and through any financial institution, in violation of Title 31, United States Code, Sections 5363 and 5366.

Overt Acts

51. In furtherance of the conspiracy and to effect the illegal object thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about October 1, 2007, by email, CC-1 informed another individual that his internet casino "is one of the only casinos accepting players worldwide including the United States."

b. On or about January 13, 2010, by email, CC-1 arranged to send advertisements promoting CC-1's internet casinos by U.S. mail to up to one hundred thousand U.S. residents in over 30 states, including the Southern District of New York.

c. On or about December 8, 2013, CC-3, by email, informed CC-1 that "casino turnover" for the month of October 2013 was $78,910,099, which was "almost no change" from a given

month approximately one year earlier, July 2012, when monthly "casino turnover" was $75,259,052.

d. On or about May 8, 2014, at CC-1's direction, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, provided the login credentials for various individuals who owned or worked at Victim-10 and Victim-11.

e. Between approximately June 26, 2015, and July 7, 2015, in the Southern District of New York and elsewhere, a federal law enforcement agent, acting in an undercover capacity, deposited U.S. currency and gambled at one of CC-1's internet casinos.

(Title 18, United States Code, Section 371.)

COUNT NINE

(Conspiracy to Commit Wire Fraud and Bank Fraud: Unlawful Payment Processing)

The Grand Jury further charges:

52. The allegations contained in paragraphs 1 through 28, 33, 47, and 51 of this Indictment are repeated and realleged as if fully set forth herein.

53. From at least in or about 2011, up to and including on or about July 2015, in the Southern District of New York and elsewhere, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, willfully and knowingly combined,

conspired, confederated, and agreed together and with each other to violate Title 18, United States Code, Sections 1343 and 1344.

54. It was a part and an object of the conspiracy that ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud, and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343, to wit, TYURIN and his co-conspirators participated in a scheme involving wire communications to deceive financial institutions and other financial intermediaries into processing and authorizing payments to and from (i) various gambling businesses and United States gamblers, (ii) distributors of unlicensed pharmaceuticals around the world, and (iii) purveyors of counterfeit and malicious purported anti-virus software in the United States, by disguising the transactions to create the false appearance that they were unrelated to gambling, unlicensed pharmaceutical distribution, and sales of counterfeit and malicious software,

respectively, and thereby to obtain money of, or under the custody and control of, those financial institutions and intermediaries.

55. It was a further part and an object of the conspiracy that ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, and others known and unknown, willfully and knowingly, would and did execute and attempt to execute a scheme and artifice to obtain moneys, funds, credits, assets, securities, and other property owned by, and under the custody and control of, financial institutions, the deposits of which were then insured by the Federal Deposit Insurance Corporation, by means of false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344, to wit, TIURIN and co-conspirators not named herein knowingly made, and caused other individuals to make, material misrepresentations to federally insured financial institutions and other financial intermediaries in order to deceive those financial institutions into processing and authorizing payments to and from (i) various gambling businesses and United States gamblers, (ii) distributors of unlicensed pharmaceuticals around the world, and (iii) purveyors of counterfeit and malicious purported anti-virus software in the United States, by disguising the transactions to create the false appearance that they were

unrelated to gambling, unlicensed pharmaceutical distribution, and sales of counterfeit and malicious software, respectively, and in doing so, obtained and attempted to obtain moneys, funds, and property owned by and under the custody and control of such financial institutions.

(Title 18, United States Code, Section 1349.)

FORFEITURE ALLEGATIONS

56. As a result of committing one or more of the offenses alleged in Count One and Counts Three through Six of this Indictment, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(B) any property constituting, or derived from, proceeds obtained directly or indirectly as a result of the offenses alleged Count One and Counts Three through Six and, pursuant to Title 18, United States Code, Section 1030(i), any interest in any personal property that was used or intended to be used to commit or facilitate the commission of the offenses alleged in Count One and Counts Three through Six, and any property, real or personal, constituting or derived from any proceeds obtained directly or indirectly as a result of the offenses alleged in Count One and Counts Three through Six, including but not limited to a sum of money in

United States currency representing the amount of proceeds traceable to the commission of said offenses.

57. As a result of committing the offenses alleged in Counts Two and Nine of this Indictment, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 982(a)(2)(A), any and all property constituting or derived from, proceeds obtained directly or indirectly, as a result of the commission of the offenses alleged in Counts Two and Nine of this Indictment, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

58. As a result of committing one or more of the offenses charged in Counts Seven and Eight of this Indictment, ANDREI TYURIN, a/k/a "Andrei Tiurin," the defendant, shall forfeit to the United States, pursuant to Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section 2461, any and all property, real and personal, which constitutes or is derived from proceeds traceable to the offenses alleged in Counts Seven and Eight, including but not limited to a sum of money in United States currency representing the amount of proceeds traceable to the commission of said offenses.

Substitute Assets Provision

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

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

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

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 subdivided without difficulty;

it is the intent of the United States, pursuant to Title 18, United States Code, Section 982(b), Title 21, United States Code, Section 853(p), and Title 28, United States Code, Section 2461, to seek forfeiture of any other property of the defendant up to the value of the above forfeitable property.

(Title 18, United States Code, Sections 981, 982 & 1030;
Title 21, United States Code, Section 853; and
Title 28, United States Code, Section 2461.)

[redacted]

FOREPERSON

JOON H. KIM
Acting United States Attorney

Form No. USA-33s-274 (Ed. 9-25-58)

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA

- v. -

ANDREI TYURIN,

Defendant.

SEALED SUPERSEDING INDICTMENT

S3 15 Cr. 333 (LTS)

(18 U.S.C. §§ 371, 1030, 1343, 1349, & 2)

JOON H. KIM
Acting United States Attorney.

TRUE BILL

FOREPERSON