IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA	Criminal Indictment
v.	No. **1 15 - C R - 3 9 3**
GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, AND JOHN DOE.	**Under Seal**

THE GRAND JURY CHARGES THAT:

COUNT ONE
(Wire Fraud Conspiracy)

1. Beginning on an unknown date, but at least by in or about November 2012, and continuing through in or about August 2014, in the Northern District of Georgia and elsewhere, the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, together and with others known and unknown to the Grand Jury, did knowingly conspire to devise and intend to devise a scheme and artifice to defraud financial institutions and other companies, and to obtain money and property from those financial institutions and companies, including the confidential personal identifying information of customers, 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, did with intent to defraud cause the transmission by means of wire communication in interstate and foreign

commerce of certain writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Section 1343.

BACKGROUND

2. At all times relevant to this Indictment:

a. Defendants GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE conspired together and with others to hack into the computers of E*TRADE Financial Services Corporation and its subsidiaries ("E*TRADE"), Scottrade Financial Services, Inc. and its subsidiaries ("Scottrade"), and other financial institutions and companies located in the United States, to maintain unauthorized access to those computers, and to steal personal identifying information from customer databases at those institutions for the purpose of building their own competing database for marketing and brokering stock transactions. During the course of the scheme, the defendants compromised the personal information of more than 10 million customers at E*TRADE and Scottrade alone.

b. Defendant GERY SHALON, a/k/a Garri Shalelashvili, was a resident of Israel. SHALON operated or was otherwise affiliated with several internet-based companies, including securities trading firms.

c. Defendant JOSHUA SAMUEL AARON was a United States citizen and resident of Israel and the United States. At SHALON's request, AARON provided SHALON with customer login credentials to several financial institutions targeted for attack, which SHALON sent to JOHN DOE to assist him

in locating customer databases on the large computer networks that were hacked.

d. Defendant JOHN DOE was a computer hacker who is believed to have resided in Russia. Under SHALON's direction, JOHN DOE infiltrated computer networks at these financial institutions and companies, located the customer databases, and exported the customer profile information to computers overseas.

e. E*TRADE is a financial services company headquartered in New York, New York that operates an online discount stock brokerage service. E*TRADE maintains computer servers located in the Northern District of Georgia and other locations in the United States that contain customer databases. These databases store personal identifying information of E*TRADE customers, including names, residential addresses, phone numbers, and email addresses. This customer information was confidential and economically valuable business information for E*TRADE, and the company stored the information on restricted, nonpublic servers in the United States.

f. Scottrade is a financial services company headquartered in Town and Country, Missouri that operates an online discount stock brokerage service. Scottrade maintains customer databases that store personal identifying information of its customers, including names, residential addresses, phone numbers, and email addresses. This customer information was confidential and economically valuable business information for Scottrade, and the company stored the information on restricted, nonpublic servers in the United States.

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy for defendants GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE to steal confidential customer information from financial institutions and other companies that would be valuable for compiling a database of potential investors in order to broker stock transactions. In a series of communications through an internet instant messaging service, SHALON and JOHN DOE discussed the plan to steal customer information for the purpose of making "cold calls" to potential investors to encourage them to purchase stocks through SHALON. For example, in one online chat on or about September 8, 2013 with JOHN DOE, which was originally in Russian, SHALON explained that "I read about a dude how he started the largest financial company in the world[,] this Merrill Lynch. He was making cold calls to people, offering them stocks. He would take a small percentage for the service. And it became the largest broker company in the world, that is worth, say, dozens of billions [of dollars]." When JOHN DOE asked what SHALON thought about Merrill Lynch, SHALON explained, "I kinda wanna try to see if I can get lucky with the [customer] databases to make money on cold calls. Here is what I am thinking about. If we have the databases and we sell stocks and make money, we can then suggest to a bank to buy us out."

4. In that same online conversation, SHALON discussed with JOHN DOE his plan to staff a small call center to "cold call" investors, to obtain a securities license, and to invite investment experts "to teach us how to talk properly to the

4

investors over the phone." SHALON expressed his hope that "[t]hat could be our biggest business to-date."

5. In another online chat with SHALON in September 2013, JOHN DOE proposed using a "brute-force attack," a method of hacking in which a program systematically checks all possible passwords until the correct one is found, to break into email accounts located in a victim company's customer database and determine what investment subscriptions customers were reading. SHALON expressed interest in the idea and suggested that they could use the information to "custom make a business plan for [the investors]."

6. As JOHN DOE was stealing confidential customer data from E*TRADE's restricted customer databases, SHALON discussed with JOHN DOE in another online chat on or about December 8, 2013, that he hoped to collect information on customers' trading positions so the co-conspirators could "know [the investors'] plans and take them there." SHALON explained that "[b]ig money can be made in that."

7. In another online chat in September 2013, SHALON reported to JOHN DOE that he "started cold-calling" customers identified from a victim company's customer database and reported that the early results were "[n]ot bad." In other online chats, SHALON repeatedly boasted to JOHN DOE about his early success in selling stock by "cold-calling" investors and told him that "people already think that we are good brokers :)."

MANNER AND MEANS OF THE SCHEME TO DEFRAUD

8. The manner and means by which the scheme and artifice to defraud was sought to be accomplished included, among others, the following:

a. GERY SHALON, a/k/a Garri Shalelashvili, sent JOHN DOE a list of financial institutions and other companies that he wanted JOHN DOE to hack, including E*TRADE and Scottrade. SHALON also provided JOHN DOE with a list of overseas computer servers, which he described as "100% anonymous" during an online chat, to use for the hacking activity that would permit the co-conspirators to attempt to mask the true identity and location of the computers from which they were connecting to the victims' computer networks.

b. Using overseas computer servers controlled by GERY SHALON, a/k/a Garri Shalelashvili, JOHN DOE gained unauthorized access to the victims' computer networks. During the E*TRADE intrusion, a computer server controlled by SHALON that was located in Egypt connected via wire communications with E*TRADE servers located in the Northern District of Georgia. After compromising administrative servers, JOHN DOE installed a specific type of malware — malicious code — called a "reverse shell," which was designed to connect with external computers from within the hacked computer network. This reverse shell program had a unique password tied to SHALON and beaconed messages to external computer servers selected from a list of overseas servers that SHALON provided to JOHN DOE.

c. After obtaining a foothold in the victims' computer networks, JOHN DOE searched the networks for customer databases at the direction of GERY SHALON, a/k/a Garri Shalelashvili. To facilitate his identification of these

6

databases, JOHN DOE asked SHALON to provide customer login credentials for the victims.

d. In response to this request, JOSHUA SAMUEL AARON asked Individual #1 to provide his customer login credentials to E*TRADE and Scottrade under false pretenses. Individual #1 provided his login credentials to AARON, who sent the credentials to GERY SHALON, a/k/a Garri Shalelashvili, who then gave the login credentials to JOHN DOE. JOHN DOE logged into Individual #1's accounts at E*TRADE and Scottrade and thereby misrepresented his identity in order to locate the confidential customer databases on E*TRADE's and Scottrade's internal networks.

e. After JOHN DOE found the customer databases on the victims' servers, he asked GERY SHALON, a/k/a Garri Shalelashvili, which data fields SHALON wanted to steal. At SHALON's direction, JOHN DOE exported personal identifying information of the victims' customers, including names, email addresses, and residential addresses, stolen from the confidential customer databases, which SHALON then downloaded.

f. At the request of GERY SHALON, a/k/a Garri Shalelashvili, an individual cleaned up and reformatted the stolen customer data exported by JOHN DOE and generated a report of the total number of customer accounts stolen. The report indicated that more than 100,000 residents of Georgia had their personal identifying information stolen from Scottrade's customer database. SHALON consolidated the reformatted stolen customer data in lengthy spreadsheets on a hard drive.

g. In executing the scheme, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE thereby misappropriated the confidential business information of the victim companies for their own use. SHALON's spreadsheets contained the personal identifying information of a substantial number of residents of the Northern District of Georgia that was stolen from E*TRADE's and Scottrade's confidential customer databases.

All in violation of Title 18, United States Code, Section 1349.

COUNTS TWO THROUGH FOUR
(Wire Fraud)

9. The Grand Jury re-alleges and incorporates by reference paragraphs 2 through 8 of this Indictment as if fully set forth herein.

10. On or about the dates listed in Column B of the table below, in the Northern District of Georgia and elsewhere, the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, aided and abetted by others known and unknown to the Grand Jury, having knowingly devised and intended to devise the aforementioned scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises as set forth in Count One of this Indictment, did with intent to defraud cause the transmission by means of wire communication in interstate and foreign commerce of certain writings, signs, signals, pictures, and sounds, that is, internet logins to the customer account of Individual #1 held in the victim company specified in Column C, from a server with the Internet Protocol address listed in Column D

8

and located in the foreign country listed in Column E, to victim servers located in the United States, for the purpose of executing and attempting to execute such scheme and artifice:

A	B	C	D	E
Count	Date	Victim	IP Address	IP Location
2	11/23/2013	Scottrade	41.77.138.54	Egypt
3	12/6/2013	E*TRADE	50.7.247.202	Czech Republic
4	12/7/2013	E*TRADE	50.7.247.202	Czech Republic

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNT FIVE
(Computer Fraud and Identity Fraud Conspiracy)

11. The Grand Jury re-alleges and incorporates by reference paragraphs 2 through 8 of this Indictment as if fully set forth herein.

12. Beginning on an unknown date, but at least by in or about November 2012, and continuing through in or about August 2014, in the Northern District of Georgia and elsewhere, the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, together and with others known and unknown to the Grand Jury, did knowingly and intentionally combine, conspire, confederate, agree, and have a tacit understanding with each other and with other persons known and unknown, to intentionally access

protected computers without authorization and exceeding authorization, and thereby obtain information from protected computers in furtherance of a criminal act in violation of the Georgia Identity Fraud statute, O.C.G.A. § 16-9-121(a)(1), that is, to willfully use and possess with intent to fraudulently use identifying information concerning a person without authorization and consent, in violation of Title 18, United States Code, Sections 1030(a)(2)(C) and 1030(c)(2)(B)(ii).

BACKGROUND

13. A brute force attack is a method of decrypting data in a cyber-attack in which a program systematically checks all possible passwords until the correct one is found.

14. A cookie is a small text file message generated by a website and stored on the web browser connected to the website, which is used to gather data about the user. A flash cookie is a specific type of persistent cookie that is stored in the user's computer by visiting a website that runs an Adobe Flash application.

15. An Internet Protocol address ("IP address") is a unique numeric address used by computers on the Internet. Every device connected to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination.

16. Remote Desktop Protocol, or "RDP," is a secure network communications protocol that allows a user to connect to a Microsoft-based server.

17. Reverse shells are a type of malicious code, or malware, designed to connect with an external computer from within a hacked computer network.

10

18. A user agent string is a line of text sent to a website from the web browser connected to the website that identifies the web browser version and operating system used to establish the connection. This information helps web servers customize behavior or content to specific browser versions.

19. A virtual private network, or "VPN," uses a public network connection, such as the internet, to connect to a secure internal network.

MANNER AND MEANS OF THE CONSPIRACY

20. It was part of the conspiracy that the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, and others employed the manner and means set forth in paragraph 8 of this Indictment to steal, possess with fraudulent intent, and use the confidential personal identifying information of customers of E*TRADE, Scottrade, and other financial institutions and companies, including the names and residential addresses of Georgia residents, for the fraudulent purpose of "cold-calling" potential investors to encourage them to purchase stocks through SHALON, as set forth in paragraphs 3 through 7 of this Indictment.

OVERT ACTS

21. In furtherance of the conspiracy, and in order to effect the purpose and objects thereof, the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, and others committed various overt acts in the Northern District of Georgia and elsewhere, including, but not limited to, the following:

a. On or about November 11, 2012, AARON asked Individual #1 to provide his customer login credentials to his E*TRADE account based on the claim that he wanted to create an online brokerage site similar to E*TRADE. Individual #1 sent AARON an email on that date providing his E*TRADE username and password, which AARON then forwarded to SHALON. Individual #1 never authorized AARON, SHALON, or anyone else to use his login credentials to hack into E*TRADE.

b. On or about that same day, an unknown co-conspirator logged into three E*TRADE developer accounts without authorization from a computer server with IP address 93.115.240.114, which was located in Romania and controlled by SHALON (the "Romanian server").

c. On or about November 13, 2012, AARON sent an email to SHALON with Individual #1's E*TRADE login credentials that stated "everything is working now."

d. From on or about November 12, 2012 through on or about November 20, 2012, an unknown co-conspirator logged into Individual #1's customer account at E*TRADE from the Romanian server. This user had the

same unique user agent string and flash cookie of the computer used in the unauthorized access of the E*TRADE developer accounts on or about November 11, 2012 and earlier logins to AARON's E*TRADE customer account in February 2012.

e. On or about November 28, 2012, an unknown co-conspirator logged into Individual #1's customer account at E*TRADE from a computer server with IP address 50.7.247.202, which was located in the Czech Republic and controlled by SHALON (the "Czech server"). This user had the same unique user agent string of the computer used in the unauthorized access of the E*TRADE developer accounts on or about November 11, 2012 and the prior logins to Individual #1's E*TRADE customer account in November 2012.

f. On or about September 1, 2013, an individual associated with SHALON registered a computer server with the IP address 197.85.7.101, which was located in South Africa (the "South African server").

g. On or about September 3, 2013, SHALON told JOHN DOE in an online chat, which was originally in Russian, that "[t]he servers are ready," and listed multiple overseas servers under his control, including the South African server. SHALON asked JOHN DOE to "confirm that all the servers are working," and JOHN DOE confirmed that the South African server functioned properly. JOHN DOE asked SHALON if the servers were "bulletproof," which is a form of web hosting that places minimal limits on the activities of their customers. In response, SHALON stated, "not really. And it depends on what kind of attack it is. But [they are] 100% anonymous."

h. On or about September 5, 2013, JOHN DOE told SHALON in an online chat that he "found passwords to scottrade.com on VPN." SHALON responded, "wow...Seriously?"

i. On or about the next day, JOHN DOE told SHALON in an online chat that he was "working" on Scottrade and found "an RDP of a simple user from their network."

j. On or about September 8, 2013, JOHN DOE told SHALON in an online chat that he was still working and "need[ed] to pick open scottrade." SHALON replied, "It will give us a very big push!" SHALON explained to JOHN DOE that they were looking for "investors' databases. . . . The investors are looking for ways to make money. . . .And we give them ways to make money."

k. Later that day, JOHN DOE reported to SHALON in an online chat that "[t]here is an antivirus on scottrade; can't do anything." He stated he could "only access one guy's comp[uter]. He has an antivirus, and no admin rights and the password will expire in nine days." JOHN DOE said we would "try something else," and SHALON agreed.

l. On or about the next day, SHALON asked JOHN DOE in an online chat, "What's with scottrade?" After JOHN DOE replied, "[n]othing yet," SHALON responded, "[w]e need to start hitting them :)."

m. On or about November 19, 2013, JOHN DOE told SHALON in an online chat, "I am working on scottrade, I am trying to get in there. Seems to be working." SHALON responded, "[y]es it will be a simple hit for us."

14

n. On or about November 22, 2013, JOHN DOE told SHALON in an online chat that he was "browsing inside the [Scottrade] network now, looking for a database." JOHN DOE said he "[n]eed[ed] an account on scottrade for me to find a user database," and SHALON responded that he would "take care of it now."

o. Later that day, JOHN DOE reported that he "[g]ot access to scottrade [employee] mail, almost all," and SHALON responded, "wow." SHALON asked, "[d]o you also have access to the admin?," and JOHN DOE said he did not. Later in the conversation, JOHN DOE repeated his request for "another scottrade account."

p. On or about that same day, JOSHUA SAMUEL AARON sent an email to Scottrade customer support requesting the activation of his customer account. A Scottrade representative replied by email that his request had been forwarded to a local branch office for review and processing.

q. On or about that same day, AARON contacted Individual #1 and requested that he open a Scottrade account and provide the login credentials to AARON. Individual #1 agreed to do so, and he opened an online Scottrade account and sent the login credentials to AARON. In an online chat with AARON that day, Individual #1 stated, "bout to walk into dinner. [Y]ou cool w[ith] scottrade info or need any other info?" AARON did not tell Individual #1 the true purpose for requesting his login credentials, and Individual #1 never authorized AARON, SHALON, or anyone else to use his login credentials to hack into Scottrade.

15

r. Later that day, AARON sent an email to SHALON with the subject line "login details" and the message "checked it and it works." AARON's email included a web link to a private note that would automatically delete upon being read.

s. On or about November 23, 2013, SHALON wrote to JOHN DOE in an online chat, "[p]artner, here are the details for socttrade [*sic*]" and provided the login credentials of Individual #1, including the login identification number, password, and answers to four security questions. JOHN DOE thanked SHALON for the login information.

t. On or about that same day, JOHN DOE logged into Individual #1's Scottrade account without authorization from a computer server with IP address 41.77.138.54, which was located in Egypt and controlled by SHALON (the "Egyptian server").

u. Less than an hour after thanking SHALON for providing Individual #1's login credentials to Scottrade, JOHN DOE located Scottrade's customer database and reported to SHALON in an online chat, "6 mil users there approx."

v. On or about the next day, SHALON replied, "Fuck that's a shitload :)," and asked what data fields were visible. JOHN DOE provided a full list of data fields in Scottrade's confidential customer database, including names, email addresses, residential addresses, and phone numbers. JOHN DOE stated that he was "downloading," but "it's dangerous" because a Scottrade administrator connected to the same server. SHALON requested credit card information and trade portfolios for the customers so "they will know that we know info about

16

them for real, and they will trust us more." JOHN DOE responded that he did not see credit card information.

w. Later in the conversation, JOHN DOE explained that he "[g]ot lucky with scottrade" because he took users' logins from an affiliate website "and they worked for the VPN. . . . When there is a lot of users, it is a serious problem, their passwords. Using the same ones everywhere." SHALON replied, "[t]hat's good for us :)."

x. On or about the same day, JOHN DOE uploaded four files containing personal identifying information of customers stolen from Scottrade's database and provided SHALON with the password to access the files in an online chat. SHALON replied, "I downloaded, uploading."

y. On or about November 25, 2013, SHALON sent JOHN DOE in an online chat a report based on the customer data stolen from Scottrade. This report broke down the number of customers whose data was stolen by state, including over 100,000 residents of Georgia, and listed the number of new Scottrade accounts created by month since 2006. The report indicated that the personal identifying information of at least four million Scottrade customers was compromised in the attack.

z. On or about the same day, JOHN DOE told SHALON in an online chat that Scottrade also had a bank database, and SHALON asked, "can we get it?" JOHN DOE reported to SHALON that he uploaded data for approximately 200,000 to 300,000 bank customers for SHALON in a file.

aa. On or about November 27, 2013, JOHN DOE reported to SHALON that he stole additional customer data from Scottrade and uploaded it to a file for SHALON's access.

bb. On or about that same day, SHALON shared with JOHN DOE in an online chat another report based on the customer data stolen from Scottrade that listed the data fields obtained from Scottrade, including names and email addresses. The report showed that just over six million records were stolen from Scottrade.

cc. On or about November 28, 2013, JOHN DOE conducted a brute force attack and hacked into a video teleconferencing server on E*TRADE's network, which was located in the Northern District of Georgia. He then installed malware on E*TRADE's server that permitted him to maintain access to the network.

dd. On or about November 29, 2013, JOHN DOE asked SHALON in an online chat, "what other stock market sites did you ask to look at earlier?" and mentioned E*TRADE among other victim companies.

ee. On or about December 1, 2013, JOHN DOE compromised another internal server on E*TRADE's network, which was located in the Northern District of Georgia, and installed malware that assisted his effort to scan the network and perpetrate the hack, including a reverse shell program with a unique password tied to SHALON. On or about that day, JOHN DOE reported to SHALON in an online chat, "[o]n etrade, I got into their local network. But so

far, everything is complicated." SHALON replied, "Wow, you are incredible. . . . This is good super good news."

ff. JOHN DOE conducted the initial intrusion into E*TRADE's network from the same Egyptian server used to log into Individual #1's Scottrade account on November 23, 2013.

gg. On or about December 4, 2013, JOHN DOE told SHALON in an online chat that he had not yet infiltrated E*TRADE's administrative servers "but just some device," and complained again that "[e]verything is complicated there." SHALON responded, "[b]astards, making us sweat."

hh. On or about December 5, 2013, JOHN DOE infiltrated three more internal servers on E*TRADE's network, including a core administration platform, which were located in the Northern District of Georgia. Additionally, the reverse shell program that JOHN DOE installed on E*TRADE's compromised servers began beaconing messages to the South African server controlled by SHALON, which showed that gigabytes of data was being transferred from E*TRADE's network from on or about December 5, 2013 through on or about December 15, 2013.

ii. On or about the next day, JOHN DOE reported to SHALON in an online chat, "I seem to have broken in successfully already ☺," and SHALON responded, "wow that's so cool." JOHN DOE told SHALON that he "need[ed] a user on etrade," and SHALON provided him with the username and password for Individual #1's E*TRADE account, which had been provided to SHALON in

19

November 2012 by AARON. JOHN DOE thanked SHALON and stated that he was "[f]iguring things out."

jj. JOHN DOE logged into Individual #1's E*TRADE customer account from the Czech server on or about December 6, 2013 and the following day. These logins had the same unique user agent string as the login to Individual #1's Scottrade account on or about November 23, 2013 during the intrusion into Scottrade.

kk. On or about December 7, 2013, JOHN DOE told SHALON in an online chat that he "found a database :)" containing 15 million customer records and provided a snapshot image of a customer database that reflected Individual #1's email address. SHALON responded, "wow…Unfuckingbelievable…You made it?" JOHN DOE reported that he was downloading the confidential customer data.

ll. On or about the next day, JOHN DOE stated in an online chat with SHALON that he "downloaded some info…email full addr name…Phone." SHALON praised JOHN DOE as "a genius. How did you do etrade lol…It's magical."

mm. On or about December 10, 2013, JOHN DOE told SHALON in an online chat, "I will be uploading etrade now" and provided SHALON with a file name containing the customer data. SHALON responded, "Ok, downloading."

nn. On or about December 15, 2013, JOHN DOE reported to SHALON in an online chat that he uploaded additional confidential E*TRADE customer data in a new file.

oo. On or about the next day, SHALON sent JOHN DOE in an online chat a report based on the customer data stolen from E*TRADE. This report broke down the number of customers whose data was stolen by country and listed the number of new E*TRADE accounts created by month since 2000. The report indicated that at least 15 million names, email addresses, residential addresses, and phone numbers belonging to E*TRADE customers were compromised in the attack, including over 7 million unique records.

pp. After downloading the confidential customer data stolen from Scottrade and E*TRADE and reformatting the data for use, SHALON consolidated excerpts of the reformatted stolen customer data from Scottrade and E*TRADE in lengthy spreadsheets on his hard drive.

All in violation of Title 18, United States Code, Section 371.

COUNT SIX
(Computer Fraud and Abuse)

22. The Grand Jury re-alleges and incorporates by reference paragraphs 2 through 8 and paragraphs 13 through 21 of this Indictment as if fully set forth herein.

23. Beginning on an unknown date, but at least by in or about November 2012, and continuing through in or about December 2013, in the Northern District of Georgia and elsewhere, the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, aided and abetted by others known and unknown to the Grand Jury, did intentionally access a computer, namely the private, internal networks of E*TRADE, without authorization and exceeding authorization, and thereby obtained and attempted

to obtain information from a protected computer for the purpose of commercial advantage and private financial gain, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i), and 2.

COUNT SEVEN
(Computer Fraud and Abuse)

24. The Grand Jury re-alleges and incorporates by reference paragraphs 2 through 8 and paragraphs 13 through 21 of this Indictment as if fully set forth herein.

25. Beginning on an unknown date, but at least by in or about September 2013, and continuing through in or about November 2013, in the Northern District of Georgia and elsewhere, the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, aided and abetted by others known and unknown to the Grand Jury, did intentionally access a computer, namely the private, internal networks of Scottrade, without authorization and exceeding authorization, and thereby obtained and attempted to obtain information from a protected computer in furtherance of a criminal act in violation of the Georgia Identity Fraud statute, O.C.G.A. § 16-9-121(a)(1), that is, to willfully use and possess with intent to fraudulently use identifying information concerning a person without authorization and consent, in violation of Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(ii), and 2.

COUNTS EIGHT THROUGH TEN
(Aggravated Identity Theft)

26. The Grand Jury re-alleges and incorporates by reference paragraphs 2 through 8 and paragraphs 13 through 25 of this Indictment as if fully set forth herein.

27. On or about the dates listed in Column B of the table below, in the Northern District of Georgia and elsewhere, the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, aided and abetted by others known and unknown to the Grand Jury, did knowingly transfer, possess, and use, without lawful authority, a means of identification of another person, that is, the username and password of Individual #1 for his customer account held at the financial institution identified in Column C, during and in relation to the commission of a felony, as set forth in the corresponding counts identified in Column D:

A	B	C	D
Count	Date	Bank	Associated Felony Violation
8	11/23/13	Scottrade	Conspiracy to commit wire fraud as alleged in Count 1 of this Indictment.
9	12/6/13	E*TRADE	Conspiracy to commit wire fraud as alleged in Count 1 of this Indictment.
10	12/7/13	E*TRADE	Conspiracy to commit wire fraud as alleged in Count 1 of this Indictment.

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

FORFEITURE PROVISION

26. Upon conviction of one or more of the offenses alleged in Counts One through Four of this Indictment, the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(A), and Title 28, United States Code, Section 2461(c), any and all property constituting, or derived from, proceeds obtained directly or indirectly as a result of said violations;

27. Upon conviction of one or more of the offenses alleged in Counts Five through Seven of this Indictment, the defendants, GERY SHALON, a/k/a Garri Shalelashvili, JOSHUA SAMUEL AARON, and JOHN DOE, shall forfeit to the United States, pursuant to Title 18, United States Code, Sections 982(a)(2)(B) and 1030(i), the defendants' interest in any and all personal property that was used or intended to be used to commit or to facilitate the commission of such violation, as well as any and all property constituting, or derived from, proceeds obtained directly or indirectly as a result of said violations; and

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

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

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

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

    d. has been substantially diminished in value; or

    e. has been commingled with other property which cannot be divided without difficulty;
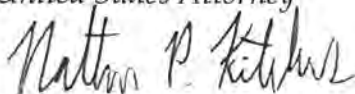
it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 18, United States Code, Section 982(b), to seek forfeiture of any other property of said defendants up to the value of the forfeitable property described above; all pursuant to Title 18, United States Code, Sections 981(a)(1)(C) and 982(a)(2)(A) & (B), and Title 28, United States Code, Section 2461(c).

A _____*TRUE*_____ BILL

_____
FOREPERSON

JOHN A. HORN
  United States Attorney

NATHAN P. KITCHENS
  Assistant United States Attorney
Georgia Bar No. 263930

600 U.S. Courthouse
75 Spring Street, S.W.
Atlanta, GA 30303
404-581-6000; Fax: 404-581-6181