ORIGINAL

Approved: _____
SARAH LAI
Assistant United States Attorney

Before: THE HONORABLE HENRY B. PITMAN
United States Magistrate Judge
Southern District of New York

18 MAG 7572

- - - - - - - - - - - - - - - - - - - -X

UNITED STATES OF AMERICA	:	SEALED COMPLAINT
-v.-	:	Violations of 18 U.S.C. §§ 1029(b)(2), 1344, 1349 and 2
JASON MICKEL ELCOCK, and SHOSHANA MARIE MCGILL,	:	
Defendants.	:	

- - - - - - - - - - - - - - - - - - - -X

SOUTHERN DISTRICT OF NEW YORK, ss.:

CARRIE CROT, being duly sworn, deposes and says that she is a Special Agent with the Federal Bureau of Investigation ("FBI") and charges as follows:

COUNT ONE

(Conspiracy to Commit Wire Fraud and Bank Fraud)

1. From at least in or about 2015, up to and including in or about September 2018, in the Southern District of New York and elsewhere, JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit wire fraud and bank fraud, in

violation of Title 18, United States Code, Sections 1343 and 1344.

2. It was a part and object of the conspiracy that JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, 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.

3. It was a further part and object of the conspiracy that JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, and others known and unknown, unlawfully, willfully, and knowingly, would and did execute and attempt to execute a scheme and artifice to defraud a financial institution, the deposits of which were then insured by the Federal Deposit Insurance Corporation, and to obtain money, funds, credits, assets, securities, and other property owned by, and under the custody and control of, such financial institution, by means of

false and fraudulent pretenses, representations, and promises, in violation of Title 18, United States Code, Section 1344.

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

COUNT TWO

(Conspiracy to Commit Access Device Fraud)

4. From at least in or about 2008, up to and including in or about September 2018, JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, and others known and unknown, willfully and knowingly combined, conspired, confederated, and agreed together and with each other to commit access device fraud, in violation of Title 18, United States Code, Section 1029(a)(5).

5. It was a part and an object of the conspiracy that JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, and others known and unknown, knowingly and with intent to defraud, would and did effect transactions, with one and more access devices issued to another person and persons, to receive payment and any other thing of value during any one-year period the aggregate value of which was equal to and greater than $1,000.

Overt Acts

6. 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 April 25, 2017, ELCOCK or MCGILL used a victim's name and credit card information without authorization in order to purchase thousands of dollars' worth of goods that were shipped to Manhattan.

b. In or about early September 2017, ELCOCK or MCGILL used another victim's account with an online marketplace to attempt to purchase a computer that was to be shipped to Manhattan.

(Title 18, United States Code, Section 1029(b)(2).)

COUNT THREE
(Bank Fraud)

7. From at least in or about 2015, up to and including in or about September 2018, JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, willfully and knowingly, executed and attempted to execute a scheme and artifice to defraud a financial institution, the deposits of which were then insured by the Federal Deposit Insurance Corporation, and to obtain money, funds, credits, assets, securities, and other property owned by, and under the custody and control of, such financial institution, by means of false and fraudulent pretenses, representations, and promises.

(Title 18, United States Code, Sections 1344 and 2.)

The bases for my knowledge and the foregoing charges are, in part, as follows:

8. I have been a Special Agent with the FBI for approximately six years. I am presently assigned to one of the Cyber Criminal Intrusion Squads of the FBI's New York Field Office. I have received training regarding computer fraud and unauthorized computer access. I have conducted numerous investigations into various forms of online criminal activity, including various fraudulent schemes perpetrated through the use of the Internet, and as such I am familiar with the ways in which such crimes are commonly conducted. In addition, I have participated in the execution of search warrants involving electronic evidence relating to those investigations, including email accounts and online storage services. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, unless noted otherwise.

OVERVIEW OF THE FRAUDULENT SCHEME

9. From at least in or about 2008, up to and including in or about September 2018, JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, and other coconspirators not named as defendants herein, participated in a conspiracy to defraud banks and retailers by using stolen personally identifying information

("PII"), bank account information, and credit and debit card data for personal financial gain. As part of the fraudulent scheme, ELCOCK and MCGILL obtained PII and financial account information belonging to other people through various illegal means. One method was to buy or trade such data with online purveyors of stolen data. Another method was to obtain, without authorization, copies of checks in order to obtain victims' account names, account addresses, and account numbers. A third method was to acquire unauthorized access to victims' email accounts and password vaults[1] in order to gather the victims' PII and login credentials for other accounts. Yet another method was to purchase information from public records databases which was then used with social engineering techniques to gather additional information about targeted victims.

10. As a further part of the fraudulent scheme, JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, ported (transferred) victims' mobile telephone numbers from the victims' phones to other phones that ELCOCK, MCGILL, or their coconspirators controlled, without the victims' authorization. ELCOCK, MCGILL, or coconspirators not named as defendants herein then used the ported numbers fraudulently to change the online profiles of victims' financial or retail consumer accounts that

[1] A password vault is a software program that keeps a number of passwords in a secure digital location.

used the ported mobile numbers for two-factor authentication[2] or transaction alerts, or to intercept two-factor authentication codes for account access. Among other things, ELCOCK, MCGILL and their coconspirators used the fraudulently altered profiles to purchase, and attempt to purchase, millions of dollars' worth of goods and services, including goods that were shipped to Manhattan, New York.

11. As a further part of the fraudulent scheme, JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, used and attempted to use the fraudulently altered profiles, or created new fraudulent profiles, for victims' bank accounts in order to transfer funds out of the victims' bank accounts and to view account information in order to manufacture counterfeit checks drawn on the victims' bank accounts.

FRAUD REPORT FROM OATH HOLDINGS, INC.

12. From speaking with another agent and reviewing a report prepared by the Electronic Crimes Investigation Team ("ECIT") of Oath Holdings, Inc. ("Oath"), I have learned that in or about September 2017, ECIT reported to the FBI that ECIT had received information from several financial institutions that a particular Yahoo account ("Subject Account-1") had been used in

[2] Two-factor authentication is an extra layer of security that requires not only a password and username, but a device that the user has with him or her that can receive an authentication code.

connection with apparent identity theft and wire fraud activity. Specifically, Subject Account-1 had been used to log in to accounts at those financial institutions without the true account holders' authorization. After receiving those unauthorized access complaints from the financial institutions, ECIT conducted an internal investigation pursuant to Oath's terms of service policy. ECIT identified numerous other Yahoo accounts that appeared to be linked directly or indirectly to Subject Account-1 based on various indicators, including, among others, the Internet protocol ("IP") addresses used to create and/or access the accounts and shared secondary email accounts or mobile phone accounts. The ECIT also identified a particular AOL email address ("Subject Account-2") that exchanged emails with Subject Account-1, at least two of which referenced credit profiles. According to ECIT, the subject lines of the emails in the Yahoo accounts that ECIT investigators identified suggested that the accounts were being used for fraud. For example, there were an unusually large number of emails from banks, including some that confirmed changes to bank account profiles.

THE INVESTIGATION

13. On or about September 14, 2017, the Honorable James L. Cott, United States Magistrate Judge for the Southern District of New York, issued a warrant (the "September 2017 Warrant") authorizing the search of email and text messages stored in

Subject Account-1 and Subject Account-2, and two other email accounts identified by ECIT: Subject Account-3 and Subject Account-4 (collectively, the "Subject Accounts"), among other accounts. The contents of the Subject Accounts, which other agents and I have searched, confirmed that they were used in furtherance of an identity theft and financial fraud scheme that began as early as 2008. For example:[3]

a. Subject Account-1 was used, among other ways, to communicate with coconspirators. For example, between on or about July 12, 2016 and July 19, 2016, the following series of email messages were sent to and from Subject Account-1:

Date	Participant	Message
7/12/16 3:56pm	Coconspirator-1 ("CC-1"):	Boa [meaning Bank of America; attached to this email message was a photo of an individual holding a phone that showed the routing and account numbers of the Bank of America account at issue]
7/18/16 1:28pm	Subject Account-1:	check the *[name redacted]* boa [meaning a Bank of America account], do not sign in online that be f*[**]*kin it up check ova phone u need a/c# and last 4 ssn 800-432-1000
7/18/16 1:54pm	Subject Account-1:	if they ask its from *[company name redacted]*
7/18/16 2:10pm	CC-1:	18 how u want me to get it out how much etc send the senders info

[3] I have included my preliminary interpretations of some of the terms used in the email and text messages which are based on my training, experience, and participation in this investigation.

7/18/16 2:50pm	Subject Account-1:	head gotta go to teller bro like 6k [meaning $6,000], go to 3 spots [meaning three different bank branches], its from *[company name redacted]*
7/18/16 5:51pm	CC-1:	grabbed 12 off oa [possibly a typographical error that was intended to read "boa"]
7/19/16 5:19pm	CC-1:	its only 2k left on it Im going to my second Mg then to nj its only here playing around everything is Gucci big bro
7/19/16 6:09pm	CC-1:	3 n change left on it [meaning the balance in the victim account after CC-1's withdrawals]

b. Subject Account-2 contained an email dated on or about February 27, 2016, with the subject line "*[name redacted]* TransUnion Personal Credit Report_20160226." Subject Account-2 was also used to send multiple emails that contained credit/debit card numbers, account names, addresses and telephone numbers, expiration dates, and card verification values. Most of these emails were sent to Subject Account-1, and the account data contained therein was shown in a format that suggested the data had been stolen from a database.

c. On or about January 9, 2008, Subject Account-3 received an email from another coconspirator not named as a defendant herein containing PII and/or account access information of approximately five individuals. Subject Account-3 also contained hundreds of text messages regarding the purchase, sale and exchange of stolen credit/debit card data and

login credentials. As an example, on or about July 3, 2013, the user of Subject Account-3 texted another coconspirator not named as a defendant herein to ask for a test card: "dude u still not gonna give me one for test?" On or about July 13, 2013, another coconspirator not named as a defendant herein texted Subject Account-3, "have some good usa dumps." Based on my training and experience, I know that credit card thieves often use the term "dump" to refer to Track 2 data (i.e., data embedded in the magnetic strips of credit and debit cards). On or about June 17, 2014, Subject Account-3 received a text message from yet another coconspirator not named as a defendant herein who offered "updated us uk ca au …! fresh here," meaning recently pilfered data for credit or debit cards issued by banks in the United States, the United Kingdom, Canada and Australia were available.

d. Subject Account-4 contained numerous emails that were addressed to another individual, but forwarded to Subject Account-4. As explained in paragraphs 20-21 and 26 below, these emails were forwarded using an automated email forwarding rule without the intended recipient's authorization.

14. Other agents and I have identified individuals whose names and PII and/or account information were found in the Subject Accounts, who appeared to be victims of identity theft. From personally interviewing some of those apparent victims and

reviewing reports of interviews conducted by other agents as well as related bank records, I learned, in substance and in part, the following:

Victim-1 and Victim-2

15. Victim-1 was an employee of a certain creative company based in Manhattan, New York (the "Victim Creative Agency"). The Victim Creative Agency maintained an account at JPMorgan Chase Bank ("Chase"), with an account number ending in 965 (the "965 Account"). Victim-2 was an employee of a financial services company who, together with Victim-1, managed accounting-related matters for the Victim Creative Agency. Both Victim-1 and Victim-2 had authorized access to the 965 Account. All Chase alerts regarding transactions in the 965 Account were supposed to be sent only to Victim-2's email address, who would forward them to Victim-1.

16. Victim-2 recalled, in substance and in part, that in or about the first week of November 2016, he received a call from his cellphone company that his mobile number that was linked to the 965 Account had been used by another telephone. Victim-1 recalled, in substance and in part, that in or about the second week of November 2016, she received a similar call from her cellular service provider regarding her cellphone that was linked to the 965 Account. Shortly after those calls, Victim-2 received a call from Chase informing him that certain

fraudulent transactions affecting the 965 Account had been stopped. Specifically, Victim-1 and Victim-2 learned that on or about November 14, 2016, one or more unidentified individuals attempted to make two unauthorized wire transfers totaling more than $47,500 from the 965 Account.

17. From reviewing emails in Subject Account-3, I know that on or about November 14, 2016, Subject Account-3 received at least two emails from Chase that began "Dear [Victim Creative Agency]." One of those emails continued, in substance and in part, "We've received your Chase Online (SM) request to update your phone information." The second email read, in substance and in part, "We have updated your online profile, based upon the information you supplied." Subject Account-3 should not have received those emails because only Victim-2's email address was supposed to receive Chase alerts. According to Chase records for the 965 Account, on or about November 8, 2016--or approximately one week before the fraudulent wire transfers--an unidentified individual created a fraudulent profile for Victim-1, with Subject Account-3 as the email address for that profile. Based on the foregoing sequence of events, I believe that the user of Subject Account-3 compromised the 965 Account by creating the fraudulent profile in order to effectuate unauthorized transactions in the 965 Account.

18. Based on my training and experience, I know that deposits in Chase accounts are insured by the Federal Deposit Insurance Corporation.

Victim-3

19. In or about the end of August 2017, Victim-3 discovered that she was unable to use her cellphone. Victim-3 contacted her cellphone carrier and learned that her cellphone number had been ported to a different carrier without her authorization. Shortly thereafter, Victim-3 received at least one email from an online marketplace notifying her that an unidentified individual had tried to buy a MacBook Pro computer using Victim-3's online shopping account, to be shipped to New York. That fraudulent purchase resulted in an unauthorized charge of approximately $3,000 to Victim-3's credit card.

20. From searching the emails in Subject Account-1, I found many emails addressed to Victim-3 that were dated from on or about August 29, 2017, and September 14, 2017. The earliest of these was an email from Yahoo which read, in substance and in part, "Hi [Victim-3], You've added [Subject Account-1] to your Yahoo account *[redacted]*." Subsequent emails appeared to have been systematically auto-forwarded to Subject Account-1 using a forwarding rule. For example, there was an August 30, 2017 email from Facebook to Victim-3's true email account which informed Victim-3 that her Facebook password had just been

changed. This email's header information contained the following forwarding rule, showing that the email had been copied to Subject Account-1:

> X-Yahoo-Forwarded: From [Victim-3's username]@yahoo.com To [Subject Account-1]

Based on my training, experience, and participation in this investigation, I believe that the user(s) of Subject Account-1 infiltrated Victim-3's email account in order to create the forwarding rule; to learn about her personal habits, such as where Victim-3 banked, what credit cards she used, where she shopped; and/or to intercept emails regarding unauthorized purchases in order to delay Victim-3's discovery of those unauthorized transactions. The information obtained from Victim-3's email account was then used to impersonate her in fraudulent online transactions.

21. As discussed above, after Victim-3's phone number was ported, she received an email regarding an unauthorized purchase of an Apple computer using her credit card. I have searched in Subject Account-1 and found that it contained three emails, dated September 1, 5, and 7, 2017, from an online marketplace with subject lines that referred to an Apple MacBook Pro computer. Header information for these emails revealed that they had been forwarded from Victim-3's true email account to Subject Account-1 with a forwarding rule:

X-Yahoo-Forwarded: From [Victim-3's username]@yahoo.com
To [Subject Account-1]

Victim-4

22. Victim-4 was a payroll manager of a company that, among other things, provided real estate-related services (the "Victim Real Estate Company"). Victim-4 stated, in substance and in part, that she had signatory authority over the Victim Real Estate Company's accounts at Chase. Victim-4 did not have an online profile for those Chase accounts; instead, Victim-4 interacted with Chase by telephone or in person. In or about May 2016, in response to Victim-4's inquiry about establishing an online profile for the Victim Real Estate Company's Chase accounts, Victim-4 learned from a Chase representative that, unbeknownst to Victim-4, she already had an online profile with her Social Security number. In addition, Victim-4 learned that her profile had been used to view checks and balances in several accounts at Chase over which she had signatory authority. Victim-4 further discovered that several fraudulent checks had been issued against those compromised Chase accounts.

23. I have reviewed Chase records which showed that on or about May 6, 2016, an unidentified individual created a fraudulent online profile in the name of Victim-4 and added Subject Account-1 as Victim-4's email address. On or about May 24, 2016, an unidentified individual used the fraudulent

Victim-4 profile to view the full routing and account numbers for a Chase business checking account held in the name of the Victim Real Estate Company, with an account number ending in 801 (the "801 Account"). Thereafter, on or about June 27, 2016, three fraudulent checks totaling approximately $6,200 were issued against the 801 Account and deposited into other Chase accounts not held in Victim-4's name at Chase branches located in Manhattan, New York. All three checks were determined to be fraudulent and the funds were reversed out of the payees' accounts.

24. Additional records produced by Chase showed that Subject Account-1 was also the email address for approximately twelve other customer accounts -- primarily business accounts -- at Chase. I recognized some of the account names from the content of the Subject Accounts and believe that at least some of them are other victim accounts. All of them have been involved in transactions that Chase designated as "fraud" or "suspicious."

Victim-5

25. Victim-5 informed me, in substance and in part, that in or about late April 2017, Victim-5 found that he was unable to use his cellphone, which he used for two-factor authentication. Victim-5 learned from his cellphone carrier that his mobile number had been ported to another cellphone

carrier, without Victim-5's authorization. Victim-5 then checked his credit card account and saw that it had been used on or about April 25, 2017, to purchase Apple laptops and gift cards at a New York branch of a major consumer electronics store ("Retailer-1"). Victim-5 also discovered that his Apple ID and email account passwords had been reset, again without his authorization.

26. I have searched Subject Account-1 and found numerous emails addressed to Victim-5 that were dated on or about April 25, 2017. Those emails all contained an auto-forwarding rule that forwarded emails intended for Victim-5's true email account to Subject Account-1. Among those emails were the following:

a. Emails from Retailer-1 indicating that an order that Victim-5 supposedly placed was ready for pickup from a Retailer-1 location in Manhattan, New York.

b. A Google email notifying Victim-5 that "[s]omeone recently signed into your Google account [true email address] and created unusual Gmail message filters."

c. An email from an online payment system that contained a verification code for a password reset.

d. An email from Apple stating that "Two-factor authentication for your Apple ID (*[redacted]*) has been turned off at your request."

27. I have also reviewed records provided by Retailer-1 and learned that Victim-5's Retailer-1 account associated with his true email address had been used to purchase approximately $3,000 of merchandise which was shipped to one of its locations in Manhattan, New York. That order was reported as fraud.

Victim-6

28. Victim-6 informed me, in substance and in part, that in or about the spring of 2017, she discovered fraudulent activity after receiving an email notification from a credit card company (the "Credit Card Company") that her credit card had been used at an eyewear store in New York. At around the same time, Victim-6 also discovered that her cellphone number had been ported without her consent to a different carrier. As a security measure, Victim-6 canceled all of her credit cards and ordered replacement cards. Victim-6 later learned that one of the replacement cards had been sent to an address in New York City without her authorization.

29. Emails in Subject Account-4 contained numerous emails intended for Victim-6 that were auto-forwarded to Subject Account-4 with a forwarding rule. Among them was an email dated March 8, 2017, from the Credit Card Company alerting Victim-6 to an attempted charge of approximately $180 at an eyeglass shop that had been rejected. That email was preceded by other emails from the Credit Card Company, addressed to Victim-6, notifying

her of an address change to her account and the shipment of a replacement card to "BROOKLYN, NY." Victim-6 did not live in New York.

Victim-7

30. Victim-7 informed me, in substance and in part, that in or about February 2017, she received an email notification from her email service provider confirming that her email password had been changed. Because Victim-7 had not changed her email password, she immediately became concerned that her financial accounts may also have been compromised. Victim-7 attempted to call a financial institution where she maintained an account ("FI-1"), only to learn that she was unable to make calls from her cellphone. Victim-7 then received another email from FI-1 alerting her to a funds transfer out of her account, which she had not authorized. That same day, Victim-7 also contacted her cellular service provider using other means and learned that her cellphone number had been ported to another carrier without her authorization.

31. I have searched Subject Account-4 and found several emails, dated February 28, 2017, from a retailer ("Retailer-2") that were intended for Victim-7. The header of the first such email read, "to [Victim-7's first name] <[Subject Account-4]>," and confirmed an account creation. That was followed by another email acknowledging an order, then another email stating that

Retailer-2 had cancelled the order because there was a problem. Based on my training, experience and participation in this investigation, I believe that the order was canceled because Victim-7 had acted quickly to freeze her financial accounts.

32. I have also searched another Yahoo email account ("Subject Account-5") with a username that was very similar to Subject Account-4. Subscriber records showed that Subject Account-4 and Subject Account-5 were created using the same IP address less than two months apart, which suggests that the two accounts were likely created by the same individual. Subject Account-5 contained an email from yet another retailer ("Retailer-3"), also dated February 28, 2017, confirming the purchase of a $2,000 Apple Store gift card that was to be sent by email to Subject Account-4, and billed to Victim-7. Victim-7 informed me that she did not recall ever purchasing that gift card.

Victim-8

33. Victim-8, who is a resident of Minnesota, informed me, in substance and in part, that on or about May 20, 2017, she discovered that her cellphone was not working. Upon calling her cellular service provider, Victim-8 learned that her number had been ported to an unknown carrier. Around the same time, Victim-8 also learned that an IP address in New York had been used to alter her personal email address without her

authorization. Victim-8 also had a Retailer-1 account. Two days after Victim-8's phone number was ported, she learned that her Retailer-1 account, which was linked to her ported phone number, had been used to make unauthorized purchases through Retailer-1's website. Despite promptly reporting the fraudulent transaction to Retailer-1, Victim-8's Retailer-1 account was not shut down for several days. Victim-8 subsequently learned from Retailer-1 that between on or about May 20, 2017, and on or about May 30, 2017, one or more unidentified individuals made dozens of completed or attempted purchases totaling more than $270,000 from Retailer-1 using Victim-8's account, resulting in an actual loss of over $26,000 to Retailer-1. Those orders had billing addresses in approximately thirty different states, even though shipping instructions showed that nearly all of the purchases were to be shipped to Retailer-1 stores in the New York City area, primarily in Manhattan.

34. A search of Subject Account-1 yielded at least one email from Retailer-1 to Victim-8 which was forwarded from Victim-8's true email account to Subject Account-1. That email began:

----------Forwarded message---------

suggesting that an unidentified individual had logged in to Victim-8's true email account and forwarded Retailer-1's email from inside Victim-8's email account to Subject Account-1.

Victim-9

35. Subject Account-2, which communicated extensively with Subject Account-1, contained a large number of emails attaching images of checks issued against numerous business and individual checking accounts, including some with Manhattan and White Plains account addresses. One such email, sent on or about July 21, 2015, from Subject Account-2 to Subject Account-1, contained an image of a check in the amount of $400 for a Citibank account ending in 732, held in the name of a law office with a Manhattan address (the "732 Account"). Citibank records for the 732 Account, which I have reviewed, showed that on or about the date that email was sent (July 21, 2015), an unidentified individual deposited a check for approximately $5,500, issued against the 732 Account, into another Citibank account ending in 269 via an automated teller machine ("ATM") and then withdrew funds from the account. The next day, Citibank returned the check because there was insufficient funds in the 732 Account. Another agent has spoken with the owner of the 732 Account and learned that the check for approximately $5,500 was fraudulent.

36. In addition to the specific victims discussed above, the Subject Accounts contained PII and financial account information relating to hundreds of victims. Moreover, as part of this investigation, other FBI agents and I have searched an online file storage account registered to Subject Account-1 (the

"Cloud Storage Account"), pursuant to a search warrant issued on November 21, 2017, by the Honorable Andrew J. Peck, United States Magistrate Judge for the Southern District of New York. Like the Subject Accounts, the Cloud Storage Account contained account login credentials, PII, and bank and credit/debit card account information belonging to over one hundred individuals and entities. Among other things, the Cloud Storage Account contained screenshots of victims' password vaults and financial account login pages. For example, one screenshot displayed the login credentials for Victim-8's credit card accounts, bank account, and retailer accounts, including the usernames and passwords of Victim-8's credit card and Retailer-1 accounts.

37. Another indicator of the scope of the conspiracy is the large number of emails from a fee-based telephone number verification service (the "Phone Verification Company") that were stored in Subject Account-1. The overwhelming majority of those emails attached spreadsheets that listed the phone numbers queried, the status of each number (e.g., valid or disconnected), the caller ID, and the carrier. Records provided by the Phone Verification Company for the account associated with Subject Account-1 revealed that the account holder queried over 10,000 phone numbers in or about 2017, and used credit cards issued to "Shoshana McGill," with an address in Brooklyn, New York, to pay for those queries. As discussed above, many of

the victims whom other agents and I have interviewed reported that their cellphone numbers had been ported without their consent at around the time that unauthorized transactions occurred in their financial accounts. Some of their phone numbers -- including those of Victim-6 and Victim-7 -- were found in the list of 10,000 phone numbers. Accordingly, I believe that the user(s) of Subject Account-1 used the information obtained from the Phone Verification Company as one way to select their victims and port their mobile numbers.

IDENTIFICATION OF THE USERS OF SUBJECT ACCOUNT-1, SUBJECT ACCOUNT-2, SUBJECT ACCOUNT-3, AND SUBJECT ACCOUNT-4

38. As discussed below, based on the content of emails in the Subject Accounts, and information from publicly available social media posts, bank records, and law enforcement databases, I believe that SHOSHANA MARIE MCGILL, the defendant, is the user of Subject Account-2; JASON MICKEL ELCOCK, the defendant, is the user of Subject Account-3 and Subject Account-4; and both ELCOCK and MCGILL are users of Subject Account-1.

SHOSHANA MARIE MCGILL is the User of Subject Account-2

39. Subscriber records produced by Oath, Inc. show that Subject Account-2 was registered on or about September 10, 2006, to "Shoshana McGill," with an address in Brooklyn, New York. I have also reviewed account opening records for a Municipal Credit Union account held in the name of "Shoshana Marie McGill"

("McGill's MCU Account") and learned that McGill listed her email address as Subject Account-2 and provided her date of birth. On or about September 28, 2016, Subject Account-2 received an email from Subject Account-1 that contained a photograph of a woman holding up a New York State driver's license in the name of "Shoshana M. McGill." The driver's license photo depicting McGill showed the same date of birth as the one that appeared on McGill's MCU Account records. I have also compared the photo and date of birth on that driver's license with New York State Department of Motor Vehicles ("DMV") records for SHOSHANA MARIE MCGILL, the defendant, and saw that they matched. Accordingly, I believe that MCGILL is the person using Subject Account-2. In the driver's license photo, MCGILL also held up a piece of paper that read "Trading BTC [Bitcoin] with *[name redacted]*." This message is consistent with the large number of cryptocurrency-related emails in Subject Account-2. While cryptocurrencies have legitimate uses, based on my training and experience, I know that individuals involved in illicit activity often use cryptocurrencies as a more anonymous way to transfer funds and launder money than bank accounts.

JASON MICKEL ELCOCK is the User of Subject Accounts-3 and -4

40. From reviewing publicly available posts in an Instagram account belonging to an individual with the screen name "shana.2.sweet," I saw a posted photograph of a male and female holding hands, with the inscription "Shoshana & Jason's Winter Glam Baby Shower." The photo was posted on a particular date in early 2016. The woman in the photo appeared to be SHOSHANA MARIE MCGILL, the defendant. The birth certificate for a child with the last name "Elcock," who was born nine days after the date on which the baby shower announcement was posted, identified "Shoshana Marie McGill," whose date of birth matched the date shown on MCGILL's driver's license, and "Jason Mickel Elcock," with a certain date of birth ("Elcock's Date of Birth"), as the parents. Accordingly, I believe that JASON MICKEL ELCOCK, the defendant, is the male depicted in the baby shower announcement and his date of birth is the one listed on his child's birth certificate.

41. Records on file with the U.S. Citizenship and Immigration Services showed that there is a "Jason Marlon Mickeal" with Elcock's Date of Birth and whose mother's name was listed as "Michele Elcock." There is also a Petition for Alien Relative filed by a "Michele Tustin Elcock" for her child "Jason Marlon Elcock" with Elcock's Date of Birth. Given the similar

names and identical date of birth, I believe that "Jason Marlon Mickeal," "Jason Marlon Elcock," and "Jason Mickel Elcock" are the same person.

42. A Facebook account registered to "Shoshana McGill," whose vanity (screen) name was "Shana2Sweet," contained a publicly available photograph of a male and a female hugging (only the back of female is shown), with the male holding a jewelry box with a ring. I believe that this photo, posted in or about November 2017, was an engagement photo. The accompanying post read, in part, "This is the moment I got to see the love of my life Jason EL on one bended knee[.]" The "Jason EL" in the photo is the same person as the "Jason Mickel Elcock" in the baby shower announcement discussed in paragraph 40 above, who I believe to be JASON MICKEL ELCOCK, the defendant.

43. "Jason EL" (including the capitalization of "EL") is the vanity name for the Facebook profile at https://www.facebook.com/prezzibk. One of the photos posted at "Jason EL's" Facebook profile showed a man wearing a baseball cap with the words "Brooklyn -vs- Everybody." The male depicted in that photo is the same person as the "Jason" in the baby shower announcement discussed in paragraph 40 above. According to subscriber records, the email address for "Jason EL's" Facebook profile is Subject Account-4. Subject Account-4

contained numerous Facebook notifications addressed variously to "Jason 'prezzi' Elcock <[Subject Account-4]>," "Jason Prezzi <[Subject Account-4]>," and "Jason EL <[Subject Account-4]>." "Prezzi" appears to be a shortened form of "prezzibk," the username for Jason Mickel Elcock's Facebook profile, and "bk" likely stands for "Brooklyn." I therefore believe that the user of Subject Account-4 is "Jason EL," who is the "Jason" in the baby shower announcement and is JASON MICKEL ELCOCK, the defendant.

44. Several emails in Subject Account-3 contained messages that began, "Dear Jason Elcock" and "Congratulations bkprezzi" or referred to the nickname "prezzi" in the body of the emails. Other emails sent to Subject Account-3 were addressed to "Mickel Elcock." Header information, in the form "prezzi <[Subject Account-3]>," revealed that the user of Subject Account-3 identified himself by the screen name "Prezzi." Given the similar names in Subject Account-3 and Subject Account-4, I believe that both accounts were used by JASON MICKEL ELCOCK, the defendant.

45. Records of online sessions also support my belief that JASON MICKEL ELCOCK, the defendant, used both Subject Account-3 and Subject Account-4. In particular, the same IP addresses were used to access these two Subject Accounts over short periods of time. Based on my training and experience, I believe

that such pattern of use indicates that the same person was using those IP addresses during those periods. The following are some examples:

a. Use of IP address 108.41.22.160 on October 15, 2016

Subject Account-3	20:11:16 (GMT)
Subject Account-3	20:11:19 (GMT)
Subject Account-3	20:18:41 (GMT)
Subject Account-4	20:19:41 (GMT)
Subject Account-4	20:19:42 (GMT)

b. Use of IP address 108.41.22.160 on October 16, 2016

Subject Account-4	19:21:48 (GMT)
Subject Account-3	19:22:50 (GMT)
Subject Account-3	19:22:53 (GMT)

c. Use of IP address 108.21.77.159 on November 7, 2016

Subject Account-4	13:32:47 (GMT)
Subject Account-3	13:34:11 (GMT)
Subject Account-4	13:42:39 (GMT)
Subject Account-4	13:42:41 (GMT)

d. Use of IP address 108.54.117.239 on March 29, 2017

Subject Account-4	01:36:02 (GMT)
Subject Account-3	01:43:21 (GMT)
Subject Account-4	01:45:09 (GMT)

ELCOCK and MCGILL Are Both Users of Subject Account-1

46. The contents of Subject Account-1 and its session logs suggest that both JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the defendants, have been using Subject Account-1. Evidence pointing to MCGILL as the user of Subject Account-1 include emails in the account that began with "Hi shoshana" or "Dear Shoshana McGill." There were also emails indicating that Subject Account-1 was used to register Bitcoin accounts, similar to many emails stored in Subject Account-2 belonging to MCGILL, but not found in other Subject Accounts used by ELCOCK.[4] Evidence indicating that ELCOCK also used Subject Account-1 include emails with the header "jason elcock <[Subject Account-1]>" as well as login data that showed that the same IP address was used to access Subject Account-1 and other accounts belonging to ELCOCK in quick succession. For example, on or

[4] Subject Account-1 also contains numerous emails addressed to other people whom I believe to be victims. For example, there are email messages from banks confirming email address changes that were intended for other people (e.g., "Dear [FirstName]"), suggesting that Subject Account-1 was added to the victims' bank account profiles without authorization. There are also email headers that show different names associated with Subject Account-1 (i.e., "[firstname lastname] <[Subject Account-1]>"). Based on my participation in this investigation, I believe that those other names are likely to be either aliases designed to conceal ELCOCK's and MCGILL's true identities, or the names of victims whose identities had been taken over and fraudulently linked to the Subject Accounts.

about November 7, 2016, the following accounts were accessed from an IP address ending in .159 at the times indicated:

Subject Account-4	13:32:47 (GMT)
Subject Account-3	13:34:11 (GMT)
Subject Account-4	13:42:39 (GMT)
Subject Account-4	13:42:41 (GMT)
Subject Account-1	13:52:20 (GMT)
Subject Account-1	13:52:23 (GMT)

ELCOCK'S AND MCGILL'S UNEXPLAINED WEALTH

47. Based on information provided by the Internal Revenue Service ("IRS") pursuant to a tax order, I know that SHOSHANA MARIE MCGILL, the defendant, filed an individual tax return (Form 1040) for tax year 2014 in which she reported having two dependents and gross income in the amount of $4,642. IRS has no record of MCGILL filing tax returns for 2015, 2016 or 2017. Instead, IRS records indicate that MCGILL had no filing requirement for those three years, suggesting that her gross annual income, as reported to the IRS by others, such as banks, was below the minimum of approximately $13,250 to $13,400 for heads of households that would have triggered a filing requirement. No Social Security number has been found for JASON MICKEL ELCOCK, the defendant, to determine whether he has filed any tax returns.

48. Despite her minimal reported income, SHOSHANA MARIE MCGILL, the defendant, had access to substantial unexplained wealth. For example:

a. Records for McGill's MCU Account, which Agent-1 has reviewed, showed that between in or about January 2017, and in or about June 2018, there were approximately 140 ATM deposits totaling over $300,000 to McGill's MCU Account, a sum that is inconsistent with her reported federal income tax status.

b. DMV records and bank records showed that from in or about October 2015, to at least in or about July 2018, MCGILL had a 2014 Mercedes-Benz Model S class sedan registered to her name, for which she made a down payment of approximately $15,000 against a purchase price of $82,900.

49. Emails in MCGILL'S Subject Account-2 also revealed spending on luxury goods. According to order and shipment confirmation emails in Subject Account-2, which another agent has reviewed, MCGILL purchased or attempted to purchase approximately $37,000 of designer clothing and leather goods between in or about November 2015 and in or about September 2017. And in or about October 2015, MCGILL paid over $2,200 for a four-night stay at a 4.5-star hotel in Miami Beach.

WHEREFORE, deponent prays that arrest warrants be issued for JASON MICKEL ELCOCK and SHOSHANA MARIE MCGILL, the

defendants, and that they be imprisoned or bailed, as the case may be.

CARRIE CROT
Special Agent
Federal Bureau of Investigation

Sworn to before me this
4TH th day of September, 2018

HONORABLE HENRY B. PITMAN
UNITED STATES MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK