RMT:TAD/DKK
F. #2014R01506

17 M 367

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK
----------X

UNITED STATES OF AMERICA

- against -

IDRIS DAYO MUSTAPHA,
also known as "Idris Mustapha,"
"Idris Day Mustapha,"
"Idris D. Mustapha,"
"Chris Brownbill," and
"Melanie Sauders,"

Defendant.

----------X

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

(18 U.S.C. §§ 371, 1956(h) and 3551 et seq.)

EASTERN DISTRICT OF NEW YORK, SS:

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

Count One: Conspiracy to Commit Unauthorized Access of Computers

On or about and between January 1, 2011 and the present, within the Eastern District of New York and elsewhere, the defendant IDRIS DAYO MUSTAPHA, also known as "Idris Mustapha," "Idris Day Mustapha," "Chris Brownbill," and "Melanie Sauders," together with others, did knowingly and intentionally conspire and agree with others to commit offenses against the United States, to wit: knowingly and with intent to defraud access, and attempt to access, one or more protected computers without authorization, and exceed authorized access, and by means of such conduct further the intended fraud and

obtain something of value, to wit: the use of a computer, information and United States currency, contrary to Title 18, United States Code, Section 1030(a)(4) and 1030(c)(3)(A).

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

Count Two: Conspiracy to Commit Money Laundering

On or about and between January 1, 2011 and the present, within the Eastern District of New York and elsewhere, the defendant IDRIS DAYO MUSTAPHA, also known as "Idris Mustapha," "Idris Day Mustapha," "Chris Brownbill," and "Melanie Sauders," together with others, did knowingly and intentionally conspire and attempt to conduct financial transactions in and affecting interstate and foreign commerce, to wit: the transfer of money from bank accounts and investment accounts belonging to victims in the United States and the extraterritorial jurisdiction of the United States, which transactions in fact involved the proceeds of specified unlawful activity, to wit: identity theft, access device fraud, unauthorized access of a protected computer, and wire fraud, in violation of Title 18, United States Code, Sections 1028, 1029, 1030 and 1343, respectively, with the intent to promote the carrying on of those specified unlawful activities and knowing that the transactions were designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership and the control of the proceeds of those specified unlawful activities, contrary to Title 18, United States Code, Sections 1956(a)(1)(A)(i) and 1956(a)(1)(B)(i).

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

The source of your deponent's information and the grounds for his/her belief are as follows:[1]

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

I. Introduction

A. Overview of the Criminal Conduct

2. The FBI is investigating the unauthorized access of bank accounts and online investment accounts held by victims in the Eastern District of New York and elsewhere. The investigation has identified an international conspiracy of individuals who

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

made money by obtaining unauthorized access to bank accounts and online trading accounts, often through "phishing."[2]

3. After obtaining unauthorized access to the victim bank accounts and online trading accounts, the criminal actors monetized the scheme in two ways. First, the criminal actors initiated unauthorized wire transfers and/or the deposit of forged checks drawn from victim accounts into "drop" bank accounts that belonged to unwitting individuals. After the illicit funds had been transferred to the drop accounts, the criminal actors either transferred the funds to different accounts in the United States or transferred the money to overseas bank accounts. Second, the criminal actors also monetized the scheme through unauthorized access and trading in online investment accounts that belonged to victims in conjunction with trading in the same stocks in "aggressor accounts" controlled by the criminal actors. By placing trades in intruded victim accounts while trading the same stocks in aggressor accounts, the criminal actors were able to artificially manipulate the prices of stocks, generating profits in the aggressor accounts and losses in the victim accounts.

---

[2] "Phishing" refers to the attempt of obtaining sensitive information, such as usernames and passwords to bank or brokerage accounts, by masquerading as a trustworthy entity in an email or other electronic communication. Phishing is typically carried out by email "spoofing" or instant messaging, and it often directs users to enter details at a fake website that is designed to appear almost identical to the legitimate one. Email "spoofing" is the creation of email messages with a forged sender address. A phishing attack might begin with a spoofed email to an individual claiming to originate from the victim's bank. That spoofed email would contain a link to a web address that would look like the login page for the same bank but would in fact be a web address controlled by the criminal actors and would harvest the victim's login and password for the criminal actors.

B. The Targets of the Investigation

4. The FBI's investigation has so far identified several individuals who are members of the criminal conspiracy described above, including the defendant IDRIS DAYO MUSTAPHA ("MUSTAPHA") and an individual referred to herein as Co-Conspirator 1.

5. MUSTAPHA is a 26-year-old male who was born in Lagos, Nigeria and currently lives in the United Kingdom ("UK").

6. Based on public source information from YouTube, MUSTAPHA is a member of BTWBC ("Built to Win Ballers Club"), an Afrobeat group that has posted multiple music videos on YouTube.[3] At least three BTWBC music videos posted on YouTube depict the defendant.

7. Records obtained from Customs and Border Protection ("CBP") show that an individual named "Idris Mustapha" presented a valid UK passport ending in -4830 ("the -4830 Mustapha Passport") to enter the United States on or about May 22, 2016, on a flight from Manchester, UK, and exited the United States on or about June 1, 2016, on a flight to Manchester, UK. The date of birth of the individual presenting the -4830 Mustapha Passport was September 24, 1990. The same individual also used the -4830 Mustapha Passport and September 24, 1990, birthday to enter the United States on or about August 2, 2016, on a flight from London, UK, and exited the United States on or about August 8, 2016. Entry photographs of the individual who presented the -4830 Mustapha Passport show an

---

[3] Afrobeat is a style of popular music that incorporates elements of African music and jazz, soul and funk.

individual who matches the photograph on the -4830 Mustapha Passport as well as the individual who goes by the name "Drizzle Lomo" on the BTWBC YouTube videos.[4]

8. CBP records show that on two occasions in 2015, the defendant presented a valid UK passport ending in –3657 (the "-3657 Mustapha Passport"), to enter and exit the United States. A November 27, 2015 entry photograph of the individual who presented the -3657 Mustapha Passport matches the individual depicted in the entry photographs associated with the -4830 Mustapha Passport and "Drizzle Lomo" on the BTWBC YouTube videos.

9. As discussed below, the FBI's investigation has established that MUSTAPHA used the email address chrisbrownbill[@]rocketmail.com, an email account hosted by Yahoo, Inc. (the "Mustapha Yahoo Account").[5]

10. On or about and between April 1, 2013, and November 16, 2016, the Mustapha Yahoo Account received hundreds of emails containing the name "Mustapha," including emails containing the name "Idris Mustapha" and/or that contained other personal identification information associated with MUSTAPHA:

a. From April 1, 2013 to January 30, 2015, the Mustapha Yahoo Account received approximately 221 emails containing the name "Mustapha." Numerous emails were addressed to "Idris

---

[4] An article published on http://authorityngr.com, dated August 12, 2016, contains a photograph of the defendant, and concerns "Drizzle Lomo's" latest single, "Just U & I." The article states that "Drizzle Lomo" graduated from the University of Bradford in West Yorkshire, UK, with a degree in information communication technology. Records from a Yahoo Inc. email account belonging to the MUSTAPHA, discussed in detail below, contain multiple references to the University of Bradford.

[5] In December 2016, the Honorable Viktor V. Pohorelsky issued a search warrant for the Mustapha Yahoo Account. The specific emails described in this section were obtained pursuant to that search warrant.

Mustapha" including: (1) a May 24, 2014 reservation at a hotel in Birmingham, UK for "Mr. Idris Mustapha"; (2) a June 23, 2014 email from PayPal to "I Mustapha" asking the recipient to "confirm your new email address"; (3) a forwarded email dated August 22, 2014 concerning an air travel reservation for "Idris Mustapha" from Rhodes, Greece, to London, UK; (4) a September 21, 2014 reservation at a hotel in Manchester, UK for "Idris Mustapha"; (5) three December 23, 2014 emails from LinkedIn, a social networking company to "Idris Mustapha" asking "Idris" to confirm his email address, welcoming "Idris" to LinkedIn, and confirming "Idris's" request to join a LinkedIn group for "prospective MBAs at Bradford University School of Management."

b. From September 1, 2015 to November 16, 2016, the Mustapha Yahoo Account received approximately 99 emails that contained the name "Mustapha," including emails addressed to "Idris Mustapha." These emails included: (1) a February 2, 2016 email to "Idris Mustapha" concerning a reservation at a lodging house in Canary Warf, UK; (2) a June 30, 2016 email from KLM airlines with the subject line "Ticket for Idris Mustapha,' with an attached electronic airline ticket from Manchester, UK to Lagos, Nigeria; (3) a July 18, 2016 email from KLM airlines with the subject line "Ticket for Idris Mustapha" with an attached electronic airline ticket from Lagos, Nigeria to Manchester, UK; and (4) a November 3, 2016 to "Idris" indicating that "you have been registered by the University of Bradford where you will be able to access your academic transcript services."

c. The Mustapha Yahoo Account contained a forwarded email, dated June 22, 2016, containing an attached document concerning an appointment for "Visa Services" in Leichester, UK, for "Idris Mustapha Dayo." The document lists the full passport number for the -4830 Mustapha Passport and the same date of birth used by MUSTAPHA to enter the United States in 2016.

11. Documents obtained from Apple show that, in April 2014, the Mustapha Yahoo Account was used to register an iPad Mini in the name of "Idris Mustapha," with a listed address at 2 Rochford Gardens, Leeds, UK (the "Mustapha Leeds Address").

12. As discussed below, MUSTAPHA worked with co-conspirators, including Co-Conspirator 1. The government's investigation has revealed that Co-Conspirator 1 controlled a Gmail account (the "Co-Conspirator 1 Gmail Account A") as well as a predecessor Gmail account (the "Co-Conspirator 1 Gmail Account B"). A review of the contents of the Co-Conspirator 1 Gmail Account A and the Co-Conspirator 1 Gmail Account B showed frequent emails between those accounts and the Mustapha Yahoo Account in furtherance of criminal schemes including conspiracy to commit unauthorized access of computers and money laundering as described in more detail below.[6]

II. Crimes Involving Drop Accounts in 2011 and 2012

13. Between January 2011 and December 2012, MUSTAPHA, Co-Conspirator 1 and others engaged in a computer fraud and money laundering conspiracy wherein MUSTAPHA and others posed as women with names such as "Melanie Sauders" and "Tracy Ben." By posing as a woman, these individuals gained the trust of unwitting men in the United States and elsewhere who believed they were involved in a legitimate romance with the "woman." After gaining the victim's trust, the defendant and others concocted elaborate stories about checks that needed to be deposited into the male victims' bank accounts and then wired elsewhere. In reality, the holders of the accounts on which those checks were drawn had not authorized the checks, and the checks themselves were

---

[6] In November 2014, the Honorable Lois Bloom issued a search warrant was obtained for Co-Conspirator 1 Gmail Account A. In November 2016, the Honorable Robert M. Levy issued an additional search warrant for Co-Conspirator 1 Gmail Account A, and a search warrant for Co-Conspirator 1 Gmail Account B.

often forged using computer editing software. The male victims' bank accounts were used as unwitting "drop" or "mule" accounts to conceal that fraudulently obtained funds were subsequently deposited into bank accounts controlled by members of the conspiracy.

A. October 2011: Victim M.K.

14. As described in this section, on or about and between October 6, 2011 and October 18, 2011, MUSTAPHA, Co-Conspirator 1 and others attempted to steal approximately $25,000 from a bank account at a U.S. financial institution known to the FBI ("Financial Institution 1") in the name of an individual whose identity is known to the FBI ("Victim M.K.") using an unauthorized check. They then sought to launder the funds through an account belonging to an apparently unwitting intermediary with the online identity "Eagle Nest."

15. On or about October 6, 2011, the Mustapha Yahoo Account forwarded a chat log between "Melanie Sauders" and an individual with the online identity "Eagle Nest" to Co-Conspirator 1 Gmail Account B. In the chat log, "Melanie Sauders" repeatedly asked "Eagle Nest" about a $25,000 check from a business "customer" had been sent to "Eagle Nest" to be deposited into his bank account. "Eagle Nest" informed "Melanie Sauders" that he had deposited the check into a newly opened account at "cfe," referring to a United States financial institution known to the FBI ("Financial Institution 2"). "Melanie Sauders" also instructed "Eagle Nest" that "when check clear you need take cash out dear and deposit cash to lawyer," adding "You go and take money and pay lawyer will give

account where to put money . . ."[7] In the same chat message, "Eagle Nest" repeatedly referred to "Melanie Sauders" as "my wife."

16. On or about October 6, 2011, an unknown individual presented a check for $25,000 drawn on a Financial Institution 1 bank account in the name of Victim M.K. at a Financial Institution 2 location. The check was made out to an individual with the initials "A.F." Information obtained from Financial Institution 1 reveals that Victim M.K. was a Financial Institution 1 client who lived in Maryland and who did not issue or authorize anyone else to issue a $25,000 check to A.F.

17. On or about October 18, 2011, the Yahoo email account melaniesauders@ymail.com (the "Sauders Yahoo Account") sent an email to Co-Conspirator 1 Gmail Account B. Information obtained pursuant to subpoena shows that the Sauders Yahoo Account was listed as an "alternate communication channel" for the Mustapha Yahoo Account, indicating that both accounts are controlled by same person. In addition, both the Mustapha Yahoo Account and the Sauders Yahoo Account communicated with Co-Conspirator 1 Gmail Account B concerning the same subjects.[8]

18. The October 18, 2011 email from the Sauders Yahoo Account to Co-Conspirator 1 Gmail Account B contained a forwarded email from

---

[7] Spelling and grammatical errors in the emails and messages reprinted in these subsections appeared in the original emails and have not been corrected.

[8] On September 25, 2015, the Mustapha Yahoo Account emailed a Yahoo account with the same exact username as Co-Conspirator Gmail Account 1, stating: "we need to talk. . . . melaniesauders@ymail.com.. come on yahoo if you can," indicating that Co-Conspirator 1 should contact the defendant, the user of the Mustapha Yahoo Account, on the Sauders Yahoo Account.

"eagleone31[@]yahoo.com," an email account that apparently belonged to the unwitting intermediary, to the Sauders Yahoo Account with the subject line: "check no go," and stated in the body of the email: "your customer screw you. The check is no good. Signature on check is not what on file at bank in texas. Dear that put the no good dear. I have scan the letter and check to you."

19. The email forwarded on October 18, 2011, had two attachments, including a scanned check from Financial Institution 1 in the name of Victim M.K. for $25,000 made out to an individual with the initials A.F. The document containing the scanned check bore an electronic stamp stating: "return reason – L Signature (S) irregular." The scanned image of the $25,000 check sent from the Sauders Yahoo Account to Co-Conspirator 1 Gmail Account B matches the scanned image of the $25,000 check in records obtained from Financial Institution 1.

B. February 2012: Victim H.K.

20. As described in this section, on or about and between February 6, 2012, and February 26, 2012, MUSTAPHA, Co-Conspirator 1 and others accessed without authorization an online account at Financial Institution 1 in the name of an individual whose identity is known to the FBI ("Victim H.K."), then attempted to move those funds through intermediary victim drop accounts to obfuscate the ultimate recipient of those funds.

21. On or about February 6, 2012, a check for $55,000, drawn on a Financial Institution 1 bank account (ending in -3508) in the name of an individual whose identity is known to the FBI ("Victim H.K."), was deposited in Santa Fe, New Mexico. The payee name on the check was for an individual whose identity is known to the FBI ("Drop Victim C.M."). Information obtained from Bank of America ("BoA") shows that on or

about February 6, 2012, the $55,000 check (#1014) was credited to a BoA account (ending in -7979) belonging to Drop Victim C.M. at a BoA branch in Santa Fe, New Mexico. Victim H.K. informed Financial Institution 1 that he/she had not written that $55,000 check and had not authorized anyone else to do so.

22. On or about February 6, 2012, Co-Conspirator 1 Gmail Account B sent an email to the Mustapha Yahoo Account with the subject line "routing," followed by the word "Negash" in the body of the email, along with the routing and account number for a bank account ending in -7973. The email also included the following street address: "2981 Lothrop Detroit MI."

23. On or about and between February 9, 2012, and February 13, 2012, a total of $52,800 was transferred from Drop Victim C.M.'s BoA account:

a. On February 9, 2012, a $4,800 wire transfer from Drop Victim C.M.'s Bank of America account was performed, via teller in Santa Fe, New Mexico. The $4,800 was wired to a BoA account ending in -7973 in the name of "Negash LLC," with an address of 2981 Lothrop Street, Detroit, Michigan. This is the same account information that was sent from the Co-Conspirator 1 Gmail Account B to the Mustapha Yahoo Account on February 6, 2012.

b. On February 15, 2012, an additional $5,000 was wired from Drop Victim C.M.'s BoA account, via teller, to the Negash LLC BoA account.

c. On February 13, 2012, $43,000 was wire transferred from Drop Victim C.M.'s BoA account to another account in Victim C.M.'s name at Century Bank. Information obtained from Century Bank indicates that on February 14, 2012, $43,000 was wired out of Victim C.M.'s account to J.P. Morgan Chase, the correspondent bank for an unidentified account at a financial institution in the U.K. whose identity is known to the FBI.[9]

---

[9] After these transfers, the original deposit of the $55,000 check into Victim

24. Information provided by Financial Institution 1 shows that, on or about February 21, 2012, a $120,000 check was debited from Victim H.K.'s account at Financial Institution 1. The check was made out to another individual whose identity is known to the FBI ("Victim F.I.").

25. On or about February 26, 2012, Co-Conspirator 1 Gmail Account B sent an email to the Sauders Yahoo Account with the subject line "yyy" and an attachment. The attachment was a screenshot of transactions within Victim H.K.'s Financial Institution 1 account that would have been viewable by one who had accessed the account online. The screenshot, which included the full Financial Institution 1 checking account number, showed that on February 7, 2012, a $55,000 check (#1014) had been "paid," and that on February 21, 2012, a $120,000 check had been "paid."

26. When interviewed by Financial Institution 1, Drop Victim C.M. stated that he had received the $55,000 check from a woman named "Melanie Sauder," whom he had met on an Internet dating site. Drop Victim C.M. stated that they had been corresponding for some time on the Internet. Drop Victim C.M. indicated that he had entered into a business relationship with "Melanie Sauder," and following this, he had received the $55,000 check by FedEx, along with instructions about what to do with the funds after depositing the check.

27. Information obtained from BoA reveals that, on or about January 9, 2012, $5,000 in cash was deposited into Drop Victim C.M.'s BoA account, the same account

---

C.M.'s BoA account was reversed when the check was revealed to be fraudulent. Victim C.M.'s Bank of America was overdrawn in the amount of $55,012. The total loss to BoA was $54,950.

into which the forged $55,000 check was deposited. On or about January 12, 2012, $4,600 was transferred from Drop Victim C.M.'s BoA account to an account at another U.K. financial institution, whose identity is known to the FBI, in the name of "Idris D. Mustaph," with an associated address in Leeds, UK.

C. March 2012: Victim B.L. and Victim G.L.

28. As described in this section, on or about and between March 6, 2012, and March 22, 2012, MUSTAPHA, Co-Conspirator 1 and others accessed without authorization an online account ending in -2596 at Financial Institution 1 (the "2596 Account") in the name of an individual whose identity is known to the FBI ("Victim B.L.") and a family member of that victim ("Victim G.L.") and attempted to steal funds from that account.

29. On or about March 14, 2012, the Mustapha Yahoo Account forwarded a series of chat messages between "Tracy Ben" and an individual whose identity is known to the FBI ("Drop Victim W.D.") to Co-Conspirator 1 Gmail Account B. In the forwarded chat conversation, "Tracy Ben" stated, in relevant part: "Honey please, tomorrow the funds would be in your account," and "I swear to God this is not a money laundering, there is no way you can send the whole funds directly to Nigeria, the only way is by using merchant account, please try to understand me, if you failed to send this funds it means the orphanage children have to suffer here for a long time." In another chat conversation between "Tracy Ben" and Drop Victim W.D. contained in the same forwarded email from the Mustapha Yahoo Account, Drop Victim W.D. asked "Tracy Ben" for "corroborating documents to give to the FBI duty agent," and indicated that his bank account had been locked because of a

check that had been deposited into it. "Tracy Ben" advised Victim W.D. to "tell them the check is from a client thats all."

30. On or about March 15, 2012, Co-Conspirator 1 Gmail Account B sent an email to the Mustapha Yahoo Account. The body of the email contained the username, password, mother's maiden name, social security number, email address, email password, IP address and birth date for Victim B.L., along with Victim B.L.'s address and the account numbers for Victim B.L.'s checking and brokerage account at Financial Institution 1. The email also included a breakdown of the total dollar value in Victim B.L.'s Financial Institution 1 accounts, including stocks and mutual funds contained therein. The final lines of the email read: "drop," followed by the name of Drop Victim W.D. and a street address in Tennessee. Based on my training and experience, this email and the information contained therein suggests MUSTAPHA and Co-Conspirator 1 had acquired personal identifying information with regard to Victim B.L. and possibly obtained unauthorized access to his/her account at Financial Institution 1.

31. Information obtained from Financial Institution 1 also shows that between March 6, 2012 and March 22, 2012, numerous unauthorized Internet-based transactions occurred within a single Financial Institution 1 account held in the name of both Victim B.L. and Victim G.L.: the -2596 Account.[10]

a. On or about March 6, 2012, $85,000 was transferred from Victim B.L.'s Financial Institution 1 IRA account to the -2596 Account.

b. On or about March 8, 2012, Financial Institution 1 received a call from Victim G.L. stating that an individual who had received an

[10] This same account number appeared in the March 15, 2012 email to the Mustapha Yahoo Account.

$80,000 check in Victim G.L.'s name had called Victim G.L. to ask if he/she had written the check, to which Victim G.L. responded that he/she had not. The $80,000 was made out to Drop Victim W.D., the individual whose name appeared in the chat conversation with "Tracy Ben," and whose name and address appeared at the bottom of the March 15, 2012 email under the word "drop."

c. Also on or about March 8, 2012, Victim G.L. received a call from another individual whose identity is known to the FBI (Drop Victim "J.J."), who informed Victim G.L. that he had received a check in the mail for $80,000 payable to him from Victim G.L.'s Financial Institution 1 account. Victim G.L. had not issued or authorized anyone else to issue the $80,000 check to Drop Victim J.J. Drop Victim J.J. made a police report, in which he indicated that he had been corresponding with, purportedly, an elderly woman from Rwanda whose daughter was in an orphanage.

d. On or about March 22, 2012, Financial Institution 1 received an online wire request that originated from Victim B.L.'s Financial Institution 1 credentials to transfer $33,500 to the Wells Fargo Bank account of an individual whose identity is known to the FBI ("Drop Victim C.R."), who lived in New Jersey. A Wells Fargo representative interviewed Drop Victim C.R., who stated that he had met a woman on the Internet named "Melanie Sauders," who was from the UK. Drop Victim C.R. stated that "Melanie Sauders" had a new business, and she had instructed Drop Victim C.R. to open a new account at Wells Fargo, which he did. Drop Victim C.R. stated he was unaware of the $33,500 wire transfer to his Wells Fargo account.

32. All of the above transactions were reversed before any losses were incurred by the relevant financial institutions. The total attempted fraud amount associated with Victim B.L.'s Financial Institution 1 account was approximately $193,500.

III. Criminal Conduct in 2013

33. In or about 2013, MUSTAPHA, Co-Conspirator 1 and others continued to engage in a series of frauds involving unauthorized access of victim accounts at various financial institutions.

A. Victims G.G. and J.G.

34. As described in this section, on or about April 22, 2013, MUSTAPHA, Co-Conspirator 1 and others accessed without authorization or spoofed an AOL email account belonging to an individual whose identity is known to the FBI ("Victim G.G.") and sent an email requesting a wire transfer from an account at a U.S. financial institution whose identity is known to the FBI ("Financial Institution 3") held in the name of Victim G.G. and his/her relative, an individual whose identity is known to the FBI ("Victim J.G.")

35. On or about April 22, 2013, the Mustapha Yahoo Account sent an email to Co-Conspirator 1 Gmail Account A with the subject line: "info." The body of the email included the business name ("The local"), "sort code,"[11] account number, IBAN number, Bank name, Bank BIC/SWIFT code and business address for a bank account at a U.K. financial institution whose identity is known to the FBI that ended in -7895 (hereinafter, the -7895 Account). The following language appeared after the -7895 Account information:

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

---

[11] A sort code is an identification number used by British and Irish banks.

36. On the same date, Co-Conspirator 1 Gmail Account A responded to the above email by sending an email with the attachment "transfer_instructions_for_uk.bmp." The attachment read, in relevant part:

> "Please wire from my account, xxxx5557, the [name redacted] Revocable Trust the sum of $225,000 to the below instructions"
>
> Thank You,
>
> [scanned signature of Victim G.G.]

Below the scanned signature of Victim G.G. was information for conducting a wire transfer to the -7895 Account.

37. Also on the same date, Co-Conspirator 1 Gmail Account A sent an email to the Mustapha Yahoo Account that included the names of Victim G.G. and Victim J.G., along with Victim G.G.'s date of birth, social security number, AOL email address, phone numbers, home address in Long Island, New York, Skype telephone number, AT&T account number, business address in Long Island, New York, the number of an account (ending in -5557) at Financial Institution 3 held in the name of Victim G.G. and Victim J.G. (the "-5557 Account"), and a detailed breakdown of the dollar value of the stock positions held in the -5557 Account. The email also included the name, email address, phone number and business address of the financial advisor at Financial Institution 3 for the -5557 Account. The first name of that advisor was "Joel," the same name contained in the Mustapha Yahoo Account's April 22, 2013, email discussed above.

38. Information obtained from Financial Institution 3 shows that on April 22, 2013, the Financial Institution 3 financial advisor mentioned above received an email from Victim G.G.'s AOL email address that contained a request for the transfer of $225,000

to the -7895 Account. The email from Victim G.G.'s AOL account contained the same attachment with wiring instructions that had been sent from Co-Conspirator 1 Gmail Account A to the Mustapha Yahoo Account. The Financial Institution 3 financial advisor contacted Victim G.G., who informed the Financial Institution 3 financial advisor that he/she had not made the wire request. No loss was incurred by Financial Institution 3.

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

39. As described in this section, on or about and between May 7, 2013, and May 9, 2013, MUSTAPHA, Co-Conspirator 1 and others stole approximately $50,000 from a Financial Institution 3 account held in the name of two individuals whose identity is known to the FBI ("Victim D.R." and "Victim K.W."), through a series of unauthorized online transactions.

40. On or about May 7, 2013, Co-Conspirator 1 Gmail Account A received an email from a financial institution whose identity is known to the FBI ("Financial Institution 4"). The text of the email was addressed to Victim D.R. and thanked that individual for opening a Financial Institution 4 account ending in -6906.

41. Information obtained from Financial Institution 4 shows that the account ending in -6906 had been funded through a transfer of approximately $260,000 in equities from Victim D.R.'s Financial Institution 3 account, which Victim D.R. held with Victim K.W. Information and documents obtained from Financial Institution 3 and Financial Institution 4 reveal that Victims D.R. and K.W. had not set up an account at Financial Institution 4 and had not initiated or authorized anyone else to initiate that transfer.

42. On or about May 9, 2013, the Mustapha Yahoo Account sent an email to Co-Conspirator 1 Gmail Account A containing wire transfer instructions for a $7,669 wire transfer to the -7895 Account previously referenced in paragraph 35 herein.

43. Information provided by Financial Institution 4 shows that, on or about May 15, 2013, multiple stock positions were liquidated in the newly created Financial Institution 4 account. Moreover, on or about May 16, 2013, an international wire in the amount of $50,000 was sent to the -7895 Account, the same account provided in the May 9, 2013 email from the Mustapha Yahoo Account to Co-Conspirator 1 Gmail Account A.

44. Financial Institution 4 ultimately reimbursed Victims D.R. and K.W. for the $50,000 wire transfer, resulting in a loss to Financial Institution 4 of approximately $50,000.

IV. Frauds Involving Online Trading: 2013 through 2016

45. On or about and between 2013 and 2016, MUSTAPHA, Co-Conspirator 1 and other co-conspirators engaged in trading securities in concert with unauthorized access of the brokerage accounts of victims.

46. In furtherance of the conspiracy, the criminal actors opened online trading accounts with various U.S.-based and foreign brokerage firms. The accounts controlled by the criminal actors were often opened in the names of other individuals—sometimes friends and associates—to create layers of separation between illegal activity conducted within the accounts and the criminal actors themselves. For simplicity, the accounts controlled by the criminal actors are called "aggressor accounts." The criminal actors used the aggressor accounts to buy and sell securities traded on United States exchanges, including thinly small cap stocks, the prices of which can be artificially

manipulated due to their low per-share prices and low trading volume. At the same time, the criminal actors obtained unauthorized access to online trading accounts that belong to unwitting victims in the Eastern District of New York and elsewhere ("victim accounts"). By trading securities within the aggressor account and the victim account at the same time, the criminal actors generated fraudulent profits at the expense of the victim accounts and the underlying brokerage firms.

A. The Defendant Opens an Online Trading Account that is Used by Co-Conspirator 1 to Trade Stocks Against Victim Accounts that Were Subjected to Unauthorized Access

47. On or about October 14, 2013, the Mustapha Yahoo Account received an email from a Gmail account that contained the name "BTWBC," the musical group of which MUSTAPHA is a member. That email contained the scanned image of a UK passport in the name of an individual whose identity is known to the FBI ("Individual 1"). Based on open source information, in addition to emails contained within the Mustapha Yahoo Account, Individual 1 appears to be friends with the defendant and a member of BTWBC.

48. On or about October 16, 2013, the Mustapha Yahoo Account received an email from a U.S.-based online investment services company headquartered in New Jersey, whose identity is known to the FBI ("Brokerage Firm 1"), with the subject line "Your [Brokerage Firm 1] Login." The email was addressed to Individual 1 and contained a unique user name and password for a Brokerage Firm 1 account.

49. Information obtained from Brokerage Firm 1 shows that, on or about October 14, 2013, a Brokerage Firm 1 account was registered using a UK passport in the name of Individual 1. Brokerage Firm 1 records contain the same scanned image of

Individual 1's UK passport, which had been sent to the Mustapha Yahoo Account on or about October 14, 2013.

50. Based on my training and experience and the forgoing, MUSTAPHA opened a Brokerage Firm 1 account in the name of Individual 1 to conceal that the defendant had actually opened the account, and that it was controlled by one or more members of the conspiracy (hereinafter, the "Conspiracy Brokerage Firm 1 Account").

51. On or about October 17, 2013, several hours after receiving the email from Brokerage Firm 1 containing the unique user name and temporary password for the Conspiracy Brokerage Firm 1 Account, the Mustapha Yahoo Account forwarded that email to Co-Conspirator 1 Gmail Account A. On or about December 6, 2013, the Mustapha Yahoo Account sent a copy of the same scanned image of Individual 1's UK passport discussed above to Co-Conspirator 1 Gmail Account A.

52. Documents obtained from Brokerage Firm 1 show that the Conspiracy Brokerage Firm 1 Account was used to buy, sell, and attempt to buy and sell millions of shares of stocks, including thinly traded smallcap stocks. The stocks traded in the Conspiracy Brokerage Firm 1 Account were many of the same stocks that have been identified by various brokerage firms as stocks that were bought and sold in victim accounts that had been subjected to unauthorized access.

53. For example, on January 7, 2014, the Conspiracy Brokerage Firm 1 Account placed buy orders for approximately 32,100 shares of a corporation whose identity is known to the FBI ("Corporation 1") at prices ranging from 0.214 per share to 0.22 per share. On or about January 17, 2014, during which time the Conspiracy Brokerage Firm 1 Account still owned 32,100 shares of Corporation 1, numerous Financial Institution 1 victim

accounts that were subjects of unauthorized access were used to purchase tens of thousands of shares of Corporation 1, at prices ranging from .30 to .36 per share. These purchases inflated the price of shares of Corporation 1. That same day, and shortly after the Financial Institution 1 victim accounts were used to artificially inflate the price of Corporation 1 shares, the Conspiracy Brokerage Firm 1 Account sold its position in Corporation 1 at prices ranging from 0.2771 per share to 0.29 per share, generating profits.

54. One of the Financial Institution 1 victim accounts used to buy over 25,000 shares of Corporation 1 on January 17, 2014, was accessed that day from an IP address that was repeatedly used to access Co-Conspirator 1 Gmail Account A. Based on my training and experience and the forgoing, there is probable cause to believe that the individual who controlled Co-Conspirator 1 Gmail Account A accessed the aforementioned victim Financial Institution 1 account without authorization to use that account to purchase the Corporation 1 shares.

55. On or about February 28, 2014, the Mustapha Yahoo Account received an email from Brokerage Firm 1 indicating that the Conspiracy Brokerage Firm 1 Account had "performed trades which violated the use of funds which are unsettled," and that "you will need to deposit funds totaling $3,702.50 by 3/04/2014 in order to avoid a free riding violation regarding those transactions." On or about March 3, 2014, the Mustapha Yahoo Account forwarded that email to Co-Conspirator 1 Gmail Account A.

56. On or about May 15, 2014, the Mustapha Yahoo Account received an email from Brokerage Firm 1 stating that there was a "cash deficiency" in the Conspiracy Brokerage Firm 1 Account that "must be addressed no later than 05/19/2014." That same day, the Mustapha Yahoo Account forwarded this email to Co-Conspirator 1 Gmail Account

A. Approximately six minutes later, Co-Conspirator 1 Gmail Account A sent an email response: "ok will sell."

B. Communications in 2015 Between The Mustapha Yahoo Account and Co-Conspirator 1 Concerning the Fraudulent Scheme

57. Beginning in January 2015, the Mustapha Yahoo Account sent emails to and received emails from Co-Conspirator 1 Gmail Account A about an individual who had given money to MUSTAPHA to "invest" in MUSTAPHA and Co-Conspirator 1's "wire job" and "stock" scheme.

58. For example, on or about January 12, 2015, the Mustapha Yahoo Account wrote Co-Conspirator 1 Gmail Account A to ask where Co-Conspirator 1 was. The email stated, in relevant part: "Can you please come online didn't see or speak you days . . . ."

59. On or about January 28, 2015, the Mustapha Yahoo Account again wrote Co-Conspirator 1 Gmail Account A to ask where Co-Conspirator 1 was. That email stated, in relevant part: "Hello bro plz talk to me don't leave me in this situation . . . ."

60. On or about January 29, 2015, Co-Conspirator 1 Gmail Account A sent two emails to the Mustapha Yahoo Account to the effect that Co-Conspirator 1 was working on getting MUSTAPHA some money using an "account." The two emails stated, in relevant part: "Bro, fuck calm down give me one fucking week to get that cash.. all is ok so far with bro account" and "so calm down..and stay at home and wait wile I show u some fucking profit."

61. On or about February 3, 2015, Co-Conspirator 1 Gmail Account A sent an email to the Mustapha Yahoo Account requesting that MUSTAPHA prepare a drop

account of the kind previously described to receive funds. The email stated, in relevant part: "Bro prepare fucking biz drop.. soon I wire your cash.. wont appear online wile I have no cash." Based on my training, experience and knowledge of the investigation, the term "biz drop" refers to a "business drop account," meaning a bank account registered in the name of a (usually fake) business that can accept wire transfers from any type of bank account. The purpose of using a business drop account to receive wire transfers is to create layers of anonymity between illegally derived funds and the ultimate recipient of the funds by using the business drop account as an intermediary account.

62. On or about February 4, 2015, the Mustapha Yahoo Account emailed Co-Conspirator 1 Gmail Account A to confirm that a drop account was ready. The email stated, in relevant part: "Ok bro. I have drop."

63. On or about February 5, 2015, Co-Conspirator 1 Gmail Account A sent an email to the Mustapha Yahoo Account asking whether the drop account prepared by MUSTAPHPA could accept a transfer directly from a Brokerage Firm 1 brokerage account. The email stated, in relevant part: "Problem is that I wana send from fucking [Brokerage Firm 1] account direct…there I doing shit? Is that ok? I will need biz drop which accept any name."

64. On or about February 5, 2015, the Mustapha Yahoo Account sent an email to Co-Conspirator 1 Gmail Account A in which he asked what kind of scheme was being used to generate the funds that Co-Conspirator 1 wanted to transfer. That email stated, in relevant part:

> Is it wire job log in or what is it? Is it stock money??? You wanna send direct here I need [financial institution] business for such..but people will think it a job…bro…unless I sent to mom

> [financial institution] personal account Cuz if I send people would Wanna eat percentage it headache now bro..and now don't have [financial institution] business account for someone close to me mom has [financial institution] personal and [financial institution] personal takes any name but personal can take any amount but sometimes from USA headache for any name sometimes lately depends. What to do now??? . . . you can send to mom [financial institution]??? It old account personal will Come I think as long clean money[.]

65. Based on my training, experience and knowledge of the investigation, the term "wire job log in" refers to using a victim's credentials to "log in" to the victim's bank or investment account without authorization. Money from the victim's bank or investment account is then wired to a separate bank account — usually a "drop" account — controlled by the criminal actors. At that point, the fraudulently obtained money is either withdrawn or wired to a different account controlled by the criminal actors, and then withdrawn. The phrase "but people will think it a job … bro," followed by "Cuz if I sent people would Wanna eat percentage," reflects the fact that if Co-Conspirator 1 were to transfer the money to a drop account, then the person who controlled the drop account would expect to receive a percentage of the amount transferred. That is because the person who controlled the drop account would understand that the transferred funds were the proceeds of illegal activity. The term "stock money" appears to refer to money derived from using an aggressor account to trade stocks while also using a victim account that has been subjected to unauthorized access to trade the same stocks, thus generating profits in the aggressor account.

66. On or about February 6, 2015, Co-Conspirator 1 Gmail Account A sent the following email to the Mustapha Yahoo Account: "Bro wait…working soon I tell.. I just wana give money to dude that all..let me see I send here or direct to u."

C. The Defendant Travels Through JFK Airport to Open a Bank of America Account and a Wells Fargo Bank Account

67. CBP records show that on or about June 22, 2015, MUSTAPHA flew from London Heathrow Airport ("Heathrow") to JFK Airport. The records show that the defendant presented the -3657 Mustapha Passport to enter the United States at JFK Airport.

68. BoA records show that on or about June 23, 2015, one day after the defendant arrived at JFK Airport, an individual opened a checking account at a BoA branch in East Orange, New Jersey, in the name of "Idris D. Mustapha" (the "Mustapha BoA Account"). The individual who opened the Mustapha BoA Account completed application forms in which he listed the -3657 Mustapha Passport as a form of identification, a date of birth of September 24, 1990, and the Mustapha Leeds Address as his permanent address.

69. Records from Wells Fargo show that on June 29, 2015, a Wells Fargo checking account was opened at a branch in Newark, New Jersey, also in the name of "Idris D. Mustapha" ("the Mustapha Wells Fargo Account"). The individual who opened the Mustapha Wells Fargo Account provided a date of birth of September 24, 1990 and the -3657 Mustapha Passport.

70. CBP records show that on June 29, 2015, the defendant flew from JFK Airport to Heathrow.

71. BoA records show that, in or about and between June 2015 and November 2015, numerous debits were made from the Mustapha BoA America Account at addresses associated with "Leeds" and for which an "international transaction fee" was charged.

72. Records obtained from Wells Fargo show that, on or about and between June 29, 2015, and November 16, 2015, the Mustapha Wells Fargo Account received an international wire transfer and a series of cash deposits made at Wells Fargo branches in Newark, New Jersey and Wilmington, North Carolina. By November 16, 2015, the Mustapha Wells Fargo Account contained $19,766.32.

73. CBP records show that, on or about November 27, 2015, the defendant arrived at JFK Airport on a flight from Manchester, UK and that he presented the -3657 Mustapha Passport to enter the United States.

74. On or about November 30, 2015, the entire account balance of the Mustapha Wells Fargo Account was withdrawn at a Wells Fargo branch. The signature on the withdrawal slip completed on November 30, 2015, appears to be the same signature that appears on the signature card signed when the Mustapha Wells Fargo Account was opened.

75. CBP records show that, on or about November 30, 2015, the same day the entire balance of the Mustapha Wells Fargo Account was withdrawn, the defendant flew from JFK back to Manchester, UK.

D. The Defendant Opens a Brokerage Account that is Used to Trade Against Victim Accounts that Were Subjected to Unauthorized Access

76. MUSTAPHA and his co-conspirators also engaged in this criminal scheme involving aggressor and victim accounts through a brokerage account at a brokerage firm based in San Diego, California, whose identity is known to the FBI ("Brokerage Firm 2").

77. On or about February 26, 2016, a brokerage account was opened in the name of "Idris Dayo Mustapha" at Brokerage Firm 2 (the "Mustapha Brokerage Firm 2

Account"). Records from Brokerage Firm 2 show that the email address associated with the Mustapha Brokerage Firm 2 Account was idrisdayomustapha[@]tutanota.com (the "Mustapha Tutanota Email Account").[12]

78. On or about March 3, 2016, the Mustapha Brokerage Firm 2 Account was funded via a $32,000 transfer from the Mustapha BoA Account.

79. On or about March 17, 2016, Co-Conspirator 1 Gmail Account received an email from the Mustapha Tutanota Email Account with the subject heading: "rdp," along with two IP addresses, the word "root" and a combination of numbers and letters that appear to be two passwords. Based on my training and experience, "rdp" refers to "remote desktop protocol," a proprietary protocol developed by Microsoft, which provides a user with a graphical interface to connect to another computer over a network connection. In other words, through rdp, one can remotely access another person's computer. Based on the content of the March 17, 2016 email, it appears that the defendant MUSTAPHA was inviting Co-Conspirator 1 to remotely access a server.

80. On or about April 18, 2016, the Mustapha Brokerage Firm 2 Account began trading stocks. To conduct trades, the Mustapha Brokerage Firm 2 Account used an order management system provided by a market data company based in Carmel, New York, whose identity is known to the FBI ("Data Company 1"). As a consequence, both Data

---

[12] Tutanota is a Germany-based email provider. According to Tutanota's website, emails sent via Tutanota can be end-to-end encrypted and such emails cannot be read by Tutanota. Tutanota also advertises that it does not track the user's IP address, and users can anonymously sign up for Tutanota accounts. Tutanota emails also can be sent without encryption.

Company 1 and Brokerage Firm 2 maintained documents and information concerning trading conducted from the Mustapha Brokerage Firm 2 Account.

81. On or about and between April 2016 and May 2016, the Mustapha Brokerage Firm 2 Account repeatedly bought and sold stocks at approximately the same time that the same stocks were bought and sold in accounts belonging to victims whose accounts had been subjected to unauthorized access. The victim accounts were held at various United States and foreign brokerage firms, including Brokerage Firm 2, Financial Institution 1, and a brokerage firm based in the Bahamas that services U.S. and foreign clients ("Brokerage Firm 3"). As a result of tandem trading in victim accounts, the Mustapha Brokerage Firm 2 Account repeatedly realized thousands of dollars of gains from this trading.

82. For example, on or about May 12, 2016, during pre-market trading hours, the Mustapha Brokerage Firm 2 Account placed a series of short sale orders of thousands of shares of a corporation whose identity is known to the FBI ("Corporation 2").[13] A "short sale" is a transaction where the seller agrees to sell a security that the seller does not presently own, and that the seller has borrowed, in order to complete the transaction. Short selling is usually motivated by the belief that a security's price will decline, enabling it to be bought back at a lower price to make a profit. During this short sale, however, the Mustapha Brokerage Firm 2 Account appears to have sold Corporation 2 stock short at an artificially high price: $3.99 per share.[14] That is because the user(s) of the Mustapha Brokerage Firm 2

---

[13] Corporation 2 is a public company whose shares are traded in United States markets.

[14] On May 11, 2016, Corporation 2 closed of $3.53 per share. $3.99 per share is approximately 11.53 % higher than the prior Corporation 2 closing price of $3.53 per share.

Account knew that the short sale offer would be purchased by a victim account, which, in this instance, belonged to a victim in Queens, New York ("EDNY Victim-1").

83. From approximately 8:03 a.m. to 8:08 a.m. on May 12, 2016, the Mustapha Brokerage Firm 2 Account executed short sale orders for 41,074 shares of Corporation 2 at $3.99 per share, for total proceeds of $163,885.26.

84. From approximately 8:03 a.m. and 8:12 a.m. on May 12, 2016, EDNY Victim-1's account purchased 49,000 shares of Corporation 2.[15]

85. From approximately 8:14 a.m. to 2:51 p.m. on May 12, 2016, the Mustapha Brokerage Firm 2 Account purchased shares of Corporation 2 at prices lower than $3.99 per share to cover his short position and realize gains.

86. Notably, the Mustapha Brokerage Firm 2 Account appears to have purchased some of the Corporation 2 shares directly from EDNY Victim-1. For example, at 8:14:13 a.m., EDNY Victim-1 sold 9,000 Corporation 2 shares at approximately $3.20 per share, and the Mustapha Brokerage Firm 2 Account purchased 8,880 shares at $3.20 at 8:14:30 a.m. Later that day, at 1:51:34 p.m., EDNY Victim-1 sold 10,000 shares of Corporation 2 at $3.50 per share and the Mustapha Brokerage Firm 2 Account purchased 10,161 Corporation 2 shares at $3.50 at 1:51:34 p.m., and an additional 1,000 Corporation 2 shares at $3.50 between 1:51:20 p.m. and 1:51:40 p.m.

---

[15] From approximately 8:03 a.m. to 8:08 a.m., EDNY Victim-1 purchased 35,000 shares of Corporation 2 at $3.99 per share, for a total cost of $139,650.00. At approximately 8:11 a.m. and 8:12 a.m., EDNY Victim-1 purchased 5,000 shares of Corporation 2 at $3.98 per share and 9,000 shares of Corporation 2 at $3.89 per share, for a total cost of $19,900 and $35,010.

87. The Mustapha Brokerage Firm 2 Account realized profits of approximately $23,467 by trading Corporation 2 on May 12, 2016, excluding trading fees and commissions.

88. EDNY Victim-1's account sustained losses of approximately $31,493 from this unauthorized use of his/her account.

89. After having sustained these losses, EDNY Victim 1 was interviewed by a representative of the United States Securities and Exchange Commission ("SEC"). EDNY Victim-1 stated, in sum and substance, that he/she had not executed any trades in Corporation 2 on May 12, 2016 and that he/she had not authorized anyone else to do so on his/her behalf. EDNY Victim-1 stated, in sum and substance, that on May 12, 2016, he/she had twice attempted to log into his/her online trading account, and on each occasion, his/her account was "locked." EDNY Victim-1 stated that he/she then called his/her broker and learned about the unauthorized trades.

90. Records obtained from Data Company 1 show that on or about May 2, 2016, ten days before the unauthorized trading discussed above, EDNY Victim 1's account at Data Company 1 was accessed from a device with a MAC address[16] that was not the MAC address from which EDNY Victim 1's account at Data Company 1 previously was accessed. The MAC address was, however, identical to the MAC address associated with the device from which the Data Company 1 account linked to the Mustapha Brokerage Firm 2 Account had been accessed on several prior occasions in 2016. Based on my training and experience,

[16] As relevant to this affidavit, a media access control ("MAC") address is a unique identification number assigned to a network interface such as a wireless or ethernet card attached to a computer.

the same computer accessing the Mustapha Brokerage Firm 2 Account also appears to have accessed EDNY Victim-1's account without authorization.

91. From in or about April 2016 to May 2016, the Mustapha Brokerage Firm 2 Account also bought and sold shares of the securities of at least seven other public companies that traded in United States markets. At the same time, United States-based account holders at Brokerage Firm 2 and Brokerage Firm 3 were subjected to unauthorized access, during which time the victim accounts were used to trade the same stocks that the Mustapha Brokerage Firm 2 Account traded. The victims, whose identities are known to the FBI, reported that they had not authorized anyone to conduct trades in the aforementioned stocks and that they had not conducted the trades.

92. During this time period, the victim accounts purchased more than $5 million (aggregate) of publicly traded stock, and the victims realized aggregate losses of nearly $300,000.

93. BoA records show that, in or about and between March 2016 and May 2016, the period in which the Mustapha Brokerage Firm 2 Account engaged in trading against victim accounts, more than $100,000 was transferred from the Mustapha Brokerage Firm 2 Account to the Mustapha BoA Account and then withdrawn.

94. WHEREFORE, your deponent respectfully requests that an arrest warrant be issued for the defendant IDRIS DAYO MUSTAPHA so that he may be dealt with according to law.

[redacted]

CARRIE CROT
Special Agent
Federal Bureau of Investigation

Sworn to before me this
25th day of April 2017

[redacted]

THE HONORABLE STEVEN L. TISCIONE
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK