AO 91 (Rev. 11/11) Criminal Complaint

AUSA Peter S. Salib (312) 697-4092
AUSA Charles W. Mulaney (312) 469-6042

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

UNITED STATES OF AMERICA

v.

DANIEL SAMUEL ETA, also known as "Captain" and "Etaoko;"
OLANIYI ADELEYE OGUNGBAIYE, also known as "DonChiChi;"
BABATUNDE LADEHINDE LABIYI, also known as "Junior;"
BARNABAS OGHENERUKEVWE EDJIEH;
SULTAN OMOGBADEBO ANIFOWOSHE, also known as "Ayinde;"
BABATUNDE IBRAHEEM AKARIGIDI, also known as "AK;"
ADEWALE ANTHONY ADEWUMI;
MIRACLE AYOKUNLE OKUNOLA; and
OLUROTIMI AKITUNDE IDOWU, also known as "Idol"

MAGISTRATE JUDGE COLE

CASE NUMBER:

18CR 818

UNDER SEAL

FILED
DEC 04 2018
THOMAS G. BRUTON
CLERK, U.S. DISTRICT COURT

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

From in or around 2016 to in or around August 2018, at Chicago, in the Northern District of Illinois, Eastern Division, and elsewhere, the defendant(s)s violated:

Code Section	*Offense Description*
Title 18, United States Code, Sections 1343 and 1349	conspired with each other, and others known and unknown, to commit a wire fraud scheme

This criminal complaint is based upon these facts:

X Continued on the attached sheet.

ANDREW JOHN INNOCENTI
Special Agent, Federal Bureau of Investigation (FBI)

Sworn to before me and signed in my presence.

Date: December 4, 2018

Judge's signature

City and state: Chicago, Illinois

JEFFREY COLE, U.S. Magistrate Judge
Printed name and Title

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ILLINOIS | ss

AFFIDAVIT

I, Andrew John Innocenti, being duly sworn, state as follows:

I. INTRODUCTION

1. I am a Special Agent with the Federal Bureau of Investigation (FBI). I have been so employed since approximately March 2015.

2. As part of my duties as an FBI Special Agent, I investigate criminal violations relating to computer crime and white collar crime, including mail, wire, and bank fraud. As a law enforcement officer, I have used a variety of methods to investigate crime, including, but not limited to, visual surveillance, suspect and witness interviews, and the use of search warrants, confidential informants and undercover operations. I have participated in the execution of multiple federal search warrants. I have also received training from the FBI to investigate crimes within an ever changing high-technology environment and have experience investigating various cyber-enabled fraud and subsequent money laundering activities.

3. I have not included in the affidavit each and every fact known to me about the matters set forth herein, but only those facts and circumstances that I believe are sufficient to establish probable cause for a criminal complaint.

4. The statements contained in this affidavit are based upon my investigation, information provided by other individuals, including sworn law enforcement officers, confidential sources, witnesses and victims, and upon my

experience and training as a federal agent and the experience and training of other federal agents.

5. All dates, times, and amounts stated herein are approximate. Summaries of written statements, text messages and recorded conversations are based on draft transcriptions from Yoruba-to-English and Pidgin English-to-English translations. In reviewing this information, I relied on the draft translations of others.

6. This affidavit is made in support of a criminal complaint charging the following defendants with conspiracy to commit a wire fraud scheme from 2016 to in or around August 2018 in violation of Title 18, United States Code, Sections 1343 and 1349:

DANIEL SAMUEL ETA ("ETA"), a.k.a "Captain," a.k.a "Etaoko,"
OLANIYI ADELEYE OGUNGBAIYE ("OGUNGBAIYE"), a.k.a "DonChiChi,"
BABATUNDE LADEHINDE LABIYI ("LABIYI"), a.k.a "Junior,"
BARNABAS OGHENERUKEVWE EDJIEH ("EDJIEH"),
SULTAN OMOGBADEBO ANIFOWOSHE ("ANIFOWOSHE"), a.k.a "Ayinde,"
BABATUNDE IBRAHEEM AKARIGIDI ("AKARIGIDI"), a.k.a "AK,"
ADEWALE ANTHONY ADEWUMI ("ADEWUMI"),
MIRACLE AYOKUNLE OKUNOLA ("OKUNOLA"), and
OLUROTIMI AKITUNDE IDOWU ("IDOWU"), a.k.a "Idol."

7. In summary, and as explained below, during the timeframe of the conspiracy, ETA communicated directly with each of the above-named codefendants and other co-conspirators to perpetrate the scheme to defraud via in-person meetings, email messages, text messages, voice calls, BlackBerry Messenger messages, and/or

other electronic communication applications. Each of the alleged victims discussed below deposited money into accounts controlled by the respective defendants, who opened the bank accounts in fake names. Information regarding each of the victims below was known by ETA, who was involved in the wire fraud scheme and the laundering of the proceeds. An outline of the defendants, and the victims with whom they communicated, is as follows:

a. DANIEL SAMUEL ETA:

   i. Mystery shopper scam of Victim C (section III.A.3);

   ii. Mystery shopper scam of Victim D (section III.A.4);

   iii. Mystery shopper scam of Victim E (section III.A.5); and

   iv. Mystery shopper scam of Victim F (section III.A.6);

b. OLANIYI ADELEYE OGUNGBAIYE:

   i. Business email compromise of Victim G (section III.B.2);

c. BABATUNDE LABIYI:

   i. Romance scam of Victim I (section III.C.1);

   ii. Romance scam of Victim J (section III.C.2);

   iii. Romance scam of Victim K (section III.C.3); and

   iv. Romance scam of Victim L (section III.C.4);

d. BARNABAS OGHENERUKEVWE EDJIEH:

   i. Romance scam of Victim M (section III.D.1);

e. SULTAN OMOGBADEBO ANIFOWOSHE:

   i. Romance scam of Victim K (section III.E.1); and

ii. Romance scam of Victim L (section III.E.2);

f. BABATUNDE IBRAHEEM AKARIGIDI:

i. Romance scam of Victim K (section III.F.1); and

ii. Romance scam of Victim N (section III.F.2);

g. ADEWALE ANTHONY ADEWUMI:

i. Romance scam of Victim O (section III.G.1); and

ii. Romance scam of Victim P (section III.G.2);

h. MIRACLE AYOKUNLE OKUNOLA:

i. Employment scam of Victim Q (section III.H.1); and

i. OLUROTIMI AKITUNDE IDOWU:

i. Business email compromise of Victim R (section III.I.1).

8. Based on returns from search warrants, subpoena returns of financial records, and other evidence, each of the transactions discussed below involved communications and/or transactions of wires in interstate and foreign commerce for the purpose of executing the scheme.

II. ONLINE SCAMS

9. In summary, and explained in more detail below, the manner and means by which the conspiracy was sought to be accomplished included, among others, the following:

a. Romance Fraud Scheme - is a scheme to defraud a victim on the internet, whereby a co-conspirator contacts a victim online and builds trust through an online romance. At some point, the co-conspirator will convince a victim to send

money to a predetermined recipient under the false pretense that the victim will either get paid back in the future or that the money being sent is part of a business transaction. On some occasions, as directed by the originator of the fraud scheme, the funds originate directly from the victim's bank account, and on other occasions money is funneled through the victim's bank account to co-conspirator bank accounts without an actual loss to these victims. Victims of the latter are commonly referred to as unwitting money mules. In coordination with ETA, among others, codefendants LABIYI, EDJIEH, ANIFOWOSHE, and ADEWUMI received proceeds from Romance Fraud Schemes. These relationships evolved through email conversations, online dating websites, text messages and telephone conversations. Eventually the conspirators that posed as the victims' online love interests requested financial assistance for various purposes. Subsequently, funds were deposited into U.S. bank accounts opened in fictitious names utilizing fake passports controlled by, among others, LABIYI, EDJIEH, ANIFOWOSHE and ADEWUMI.

b. Employment Fraud Scheme – is a scheme to defraud a victim on the internet, whereby a co-conspirator contacts a victim online and hires the victim to work from home. At some point, the co-conspirator will convince a victim to send money to a predetermined recipient under the false pretense the money being sent is part of a business transaction, turning the victim into an unwitting money mule because the funds are being funneled through the victim's account. As described below, in coordination with ETA, among other co-conspirators, codefendant AKARIGIDI received proceeds from an employment fraud scheme. These

relationships evolved through email conversations. Subsequently, funds were deposited into U.S. bank accounts opened in fictitious names utilizing fake passports controlled by, among others AKARIGIDI.

c. Mystery Shopper Fraud Scheme – is a scheme to defraud operated through the United States Mail and via email, targeting individuals to be work-from-home "Mystery Shoppers" in which the targeted individuals received mystery shopper letters explaining the "job" of the mystery shopper, financial instruments, such as United States Postal Service ("USPS") Money Orders or checks through the United States Mail, and then use the proceeds of such instruments to purportedly evaluate the services of certain money transmission services, by sending money through Western Union and Money Gram. The co-conspirators would instruct the victim to deposit checks or money orders in to their own personal bank accounts, then quickly (within a day or two) withdraw cash from their bank account and purchase money orders or wire the funds to the intended recipient in the mystery shopper letter. The targeted individuals were advised that this practice was a legitimate employment opportunity. In reality, the money orders or checks sent to the victims by the co-conspirators, were typically either counterfeit or the proceeds of another fraud scheme. Once the victim's bank was notified of the fraudulent deposit, the victim's bank would absorb the loss or require the victim to make the bank whole. As it pertains to this wire fraud scheme, ETA and OGUNGBAIYE conspired to conduct Mystery Shopper Scams utilizing multiple email accounts to defraud several victims.

ETA directed the proceeds of these scams through wire transfers to various co-conspirators, to include LABIYI.

d. Online Investment Fraud Scheme – is a scheme to defraud that is similar to the other types of online fraud discussed above, in which a victim is tricked into sending money from their bank account under false pretenses. As it pertains to investment fraud, a victim is initially contacted by a conspirator online through a social media or employment platform, such as LinkedIn, purportedly in order to invest in the victim's company. On some occasions, as directed by the originator of the fraud scheme, the funds originate directly from the victim's bank account, while on other occasions, money is funneled through the victim's bank account to co-conspirator's bank accounts. This victim in this scenario is commonly referred to as an unwitting money mule. As it pertains to this wire fraud scheme, defendants ETA and OKUNOLA conspired to defraud a victim online through an Investment Fraud Scheme and directed the proceeds to a U.S. bank account opened in a fictitious name utilizing a fake passport controlled by OKUNOLA.

e. Business Email Compromise Scheme – is a scheme that typically target businesses that regularly perform wire transfer payments. The scheme is carried out by compromising legitimate business e-mail accounts through social engineering or computer intrusion techniques to defraud the victim into transferring funds. Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The conspirators targeted the method most commonly associated

with their victim's normal business practices. ETA, OGUNGBAIYE, Co-conspirator L.M. and IDOWU, together and separately, engaged in BEC schemes and received proceeds from these schemes. The defendants executed these schemes by fraudulently obtaining email credentials, including username and password combinations, and/or "spoofing" email messages that appeared to be from an employee of a company that instruct a victim to change the existing wire instructions for a pending payment to a different bank. Per the instructions given in the fraudulent emails, the victims wired funds to accounts controlled by the co-conspirators.

10. As explained below, the purpose of conducting these schemes is to obtain money. In order to obtain and/or launder victims' funds, ETA has orchestrated a network of co-conspirators who open U.S. bank accounts in fictitious names in order to receive and move these illicit proceeds to participants of the schemes, including, but not limited to, LABIYI, EDJIEH, ANIFOWOSHE, AKARIGIDI, ADEWUMI, OKUNOLA and IDOWU.

11. For example, and as described further below, a search of ETA's cellular phones revealed text, Blackberry Messenger ("BBM") and Skype communications between co-conspirators regarding the movement and transfer of monies derived from online victims, including, but not limited to, detailed bank account information, bank transfer instructions to third party accounts around the world, email addresses, and dollar amounts. Several of these messages detailed bank account numbers associated with the fictitious names, or a variation thereof, of "Chattman Ronald Stewart,"

"Beckham Smith Dave," "Garry Jimmie Stephen," "Samuel Christopher Giles," "Charles Mark," "Johnson Collins," "Luke Johnson," "Abraham Tom," "Jacob Zack," "Roy Benson" and "Norman Isaac Williams." As set forth in more detail below, these names are fake, and were utilized to open U.S. bank accounts with fraudulent passports or other forms of governmental identification for the purpose of laundering illicitly-obtained monies derived from the aforementioned online scams. Several email accounts opened in a variation of the above-referenced fictitious names were associated with corresponding bank account opening documents. Based on my training and experience, banks typically request an email address or other contact information from an account holder, so that the bank may acknowledge the account opening, send statements, or otherwise communicate with the customer. An account holder may receive emails regarding transactions on his or her account or other records of activity.

12. In or around August 2018, law enforcement obtained court authorized search warrants for email addresses discovered within ETA's cellular phones associated with fraud, specifically the following email accounts: greenmoore55@gmail.com, gregmoore2524@gmail.com, gregmoore2424@gmail.com, olaniyiogungbaiye@gmail.com, donchichivirus@gmail.com, robbybabe1@yahoo.com, and olaniyiogungbaiye@yahoo.com. The search of those email accounts revealed, among other things, mystery shopper letters and associated responses, communications regarding email extractor tools, username and password

combinations, victim mailing lists that include personal identifying information, tracking numbers, and shipping labels.

13. It was further part of the conspiracy that the proceeds resulting from the fraud schemes were transferred and concealed by the defendants by depositing the proceeds into U.S bank accounts opened in fictitious names utilizing fake passports, as well as converting the proceeds into cash and/or money orders to eliminate the paper trail, and wiring a portion of the proceeds to overseas bank accounts, and keeping a percentage for themselves.

III. ETA'S WIRE FRAUD SCHEME CONSPIRACY COORDINATION

A. DANIEL SAMUEL ETA

1. ETA Enlisted a Co-conspirator to Work Using ETA's Identification

14. As part of the scheme to defraud, as explained below, the defendants received instructions from and/or coordinated with DANIEL SAMUEL ETA ("ETA"). ETA, a.k.a "Captain," a.k.a "Etaoko," a Lawful Permanent Resident of the United States and the head of a money laundering organization operating out of the Chicago area. ETA coordinated with co-conspirators to defraud victims online, dictated the deposit of fraudulently-obtained monies from victims to U.S. bank accounts opened by additional co-conspirators in fictitious names with fraudulent passports, and then directed the transfer of these proceeds to himself as well as co-conspirators located both in the United States and overseas, often times to Nigeria.

15. As explained below, ETA appears to have no legitimate employment or source of income. ETA falsely purported in his 2016 federal income tax return that

he worked for two companies in Minnesota as a health care provider: Company A and Company B. ETA did not work for either of these companies. ETA enlisted an unnamed co-conspirator to work at both companies posing as ETA, using ETA's name and ETA's Minnesota driver's license to justify ETA's employment in the United States in an effort to obtain U.S. citizenship.

16. Specifically, on or about April 5, 2018, law enforcement officers interviewed Victim A, the co-owner of Company A. When asked if s/he employed an individual named "Daniel Samuel Eta," Victim A confirmed that the person employed as "Daniel Samuel Eta" had been employed by Company A for approximately three to four years and worked on a full-time basis at a residential group home owned by Company A. However, when shown a photo array of multiple individuals, including ETA, Victim A stated that none of those people in the photographs worked at his/her company. Victim A then compared a photograph of the person s/he had on file as "Daniel Samuel Eta" (which was taken by the company) to a copy of ETA's Minnesota driver's license which was presented in the Company A employment application process. Victim A stated that the two individuals in the photographs were not the same person.

17. On or about April 5, 2018, law enforcement officers interviewed Victim B, the director and co-owner of Company B. When asked if s/he employed an individual named "Daniel Samuel Eta," Victim B confirmed that the person employed as "Daniel Samuel Eta" had been working for Company B since approximately January 2016. However, when shown a photo array of multiple individuals that

included ETA, Victim B stated that none of the people in the photographs worked at his/her company.

18. The next day, on or about April 6, 2018, law enforcement officers again met in person with Victim B, and presented a single photograph of the unnamed co-conspirator. S/he stated that this was the individual known to him/her as "Daniel Samuel Eta" and who worked at his/her company.

19. Further investigation into ETA's finances revealed a home purchase in or around August 2017 in Skokie, Illinois. According to Bank A, ETA utilized his fraudulent 2016 federal income tax return and 2016 W-2 and Earnings Summary from Company A and Company B to show proof of employment and income. Additionally, ETA presented multiple payroll stubs from both of these companies, with a direct deposit into ETA's Bank A account ending in 4312.

20. On or about June 16, 2018, Bank A records revealed a checking account number ending in 4312 that listed ETA as the account holder. Monthly statements for this account from March 2016 to March 2018 showed several deposits into the account on a regular basis from Company A, followed by a portion of the proceeds transferred to the aforementioned unnamed co-conspirator, indicating that ETA was receiving the payroll proceeds from an employer for whom he did not actually work and sending a portion of these funds to the unnamed co-conspirator, consistent with the description of this scheme to defraud. Accordingly, ETA was filing fraudulent tax returns and using those returns to justify his employment and income to apply for a mortgage.

2. Attribution of Devices and Email Accounts to ETA, OGUNGBAIYE, and Co-Conspirators

21. As part of this investigation, on or about February 12, 2018, at the Hartsfield-Jackson International Airport, Customs and Border Protection ("CBP") agents conducted a border search of ETA upon his return from Nigeria. CBP agents recovered, in part, two phones with SIM cards carried by ETA at the time ("ETA Phone 1" and "ETA Phone 2," collectively, "ETA's Phones").

22. After a review of ETA's Phones pursuant to a court authorized search warrant, law enforcement discovered numerous communications consistent with Mystery Shopper Scams in the phone application "TextMeUp." The user ID using the TextMeUp application was "greenmoore558101" and the name "Greg Moore." According to subpoena returns from TextMe Inc., the developer of TextMeUp, the email address associated with "greenmoore558101" was listed as greenmoore55@gmail.com. As described below, "Greg Moore" and greenmoore55@gmail.com were in communication with several people who appear to be fraud victims.

23. According to Google, Inc. account records, gregmoore2524@gmail.com was opened with telephone number XXXXXXXXX3955. According to open-source information, telephone number XXXXXXXXX3955 was associated to the username "donchichivirus" and a display name of "Olaniyi...," OGUNGBAIYE's first name. In addition, according to a court authorized search, donchichivirus@gmail.com listed a recovery email address of olaniyiogungbaiye@yahoo.com and phone number of XXXXXXXXX3955. Oath Holdings, Inc. records indicate that the registered account

name for olaniyiogungbaiye@yahoo.com was "Mr. Olaniyi Ogungbaiye." As described below, ETA and the other co-conspirators are believed to share the use of numerous email addresses in furtherance of the schemes to defraud.

24. Based on the border search and search warrant review, ETA Phone 1 was using 612-644-1746 when ETA possessed it upon his return from Nigeria on or about February 12, 2018, as described above. T-Mobile USA Inc. records indicated telephone number 612-644-1746 was registered to ETA as the subscriber.

25. According to court authorized pen register trap and trace data for ETA's telephone number 612-644-1746, between approximately April 2017 through approximately August 2018, telephone number XXXXXXXXX3955 had approximately 176 text and phone communications with ETA.

26. Based on Google records, between approximately July 16, 2015, and August 3, 2018, email accounts greenmoore55@gmail.com, gregmoore2424@gmail.com, and gregmoore2524@gmail.com sent or blind copied emails to the email account donchichivirus@gmail.com, used primarily by OGUNBAIYE, containing the greetings or mystery shopper letters, as described below.

27. Google account records indicate that email accounts greenmoore55@gmail.com, gregmoore2424@gmail.com and gregmoore2524@gmail.com are registered to "Greg Morre," "Greg Moore," and "Greg Mooore," respectively. Also, greenmoore55@gmail.com listed robbybabe1@yahoo.com as the recovery email address. The gregmoore2524@gmail.com listed

robbybaby1@yahoo.com as the recovery email address. And the gregmoore2424@gmail.com account listed greenmoore55@gmail.com as the recovery email address.

28. Additionally, greenmoore55@gmail.com listed an account registration IP address of 67.162.99.205. Apple Inc. records revealed that this same IP address was used to register the billing information for an Apple iTunes account for samueleta83@yahoo.com on or about April 20, 2015, with subscriber name "Daniel Eta."

29. Information obtained from a search warrant executed on Google, Inc. email accounts greenmoore55@gmail.com, gregmoore2424@gmail.com and gregmoore2524@gmail.com have search histories related to Skokie, Illinois, where ETA resides. For example, email account greenmoore55@gmail.com reflected an internet search on or about August 2, 2017, for "4850 Elm St., #2 Skokie, IL 60077" on the real estate website Redfin.com. Email account gregmoore2424@gmail.com reflected an internet search on or about September 30, 2017, for a Target store "near me" [Skokie, Illinois]. And email account gregmoore2524@gmail.com reflected an internet search on or about November 21, 2017, for "jobs in Skokie."

30. According to BlackBerry records, the email account robbybabe1@yahoo.com is registered as the email address associated with phone number 612-644-1746. The email account robbybabe1@yahoo.com is also discussed via text messaging to unnamed co-conspirators on ETA's Phones as the email address where third party bank account information should be sent. According to court

authorized pen register trap and trace data from on or about April 5, 2017, to the present, phone number 612-644-1746 is still in use.

31. According to court authorized pen register trap and trace data from on or about October 25, 2017, to the present, BBM PIN XXXX0638, which is the BBM PIN assigned to ETA Phone 1, is still in use.

3. Mystery Shopper Scam of Victim C

32. Based on Google records, an example of a mystery shopper scheme being perpetrated by ETA using the email account gregmoore2424@gmail.com occurred on or about September 7, 2017, when an email was sent to Victim C at Victim C's email address thanking him/her for accepting an invitation to be a mystery shopper. Additional emails were sent to Victim C from "Greg Moore" providing his contact information, telephone number XXX-XXX-6617 and text only telephone number XXX-XXX-8001. The letter informed Victim C that a check should be received on the same day for his/her first secret shopper assignment. Victim C was instructed to evaluate the employees and facilities of certain Wal-Mart and Western Union facilities. Victim C was instructed to purchase $40 worth of personal items, keep $120 for his/her commission and send the remaining funds to Individual J.D. in Dallas, Texas via Money Gram or Western Union. Victim C was encouraged to complete his/her assignment as soon as possible to increase future commissions. The letter stated that Victim C should not divulge that s/he was a secret shopper and, if asked, s/he should tell the Western Union clerk that s/he was sending money to a family member. S/he

was further instructed to send his/her evaluation report, including the money transfer information, to gregmoore2424@gmail.com and robbybabe1@gmail.com.

33. Based on search warrant returns, on or about September 15, 2017, robbybabe1@yahoo.com sent an email to gregmoore2424@gmail.com that included what appeared to be a mailing list with Victim C's name, a dollar amount of $1,490, the intended recipient, a tracking number, and a delivery date of September 15, 2017. This email was originally sent earlier the same day to robbybabe1@yahoo.com by suspected unwitting money mule Individual P.S. from Individual P.S.'s email address. Additionally, within the above-referenced email string was the original mailing list sent to gregmoore2424@gmail.com by robbybabe1@yahoo.com on or about Friday, September 8, 2017, which included Victim C's name and address.

34. Based on search warrant returns, on or about September 16, 2017, Victim C sent an email to gregmoore2424@gmail.com informing "Greg Moore" that the check was deposited into his/her bank account and Victim C's mystery shopper tasks would be completed on or about September 19, 2017. Victim C later sent another email confirming s/he had completed the mystery shopper assignment.

35. On or about September 21, 2018, law enforcement interviewed Victim C. In summary, Victim C stated that s/he sent approximately $4,000 to others at the direction of the individual using gregmoore2424@gmail.com. Victim C deposited several checks s/he received from whom s/he thought was his/her mystery shopper employer, into his/her Chase Bank account. In one example, Victim C detailed that s/he received checks in the mail, performed his/her secret shopper duties utilizing

funds from the check as instructed in the letter. Victim C reported a loss of approximately $4,000.

36. According to MoneyGram records, on or about September 16, 2017, Victim C sent a Money Gram wire in the amount of approximately $843 to Individual D.A.

37. Found within ETA's Phones, on or about September 21, 2017, were two TextMeUp communications between "Greg Moore" with the account "greenmoore558101" and Victim C's telephone number. Both messages contained Victim C's telephone number, but no message content.[1] These communications likely indicate that ETA was knowledgeable about the identity of Victim C.

4. Mystery Shopper Scam of Victim D

38. According to search warrant returns on or about September 7, 2017, gregmoore2424@gmail.com sent an email to Victim D at Victim D's email address thanking him/her for accepting an invitation to be a mystery shopper.

39. According to search warrant returns, on or about September 7, 2017, robbybabe1@yahoo.com sent an email to gregmoore2424@gmail.com that included a mailing list with Victim D's telephone number, XXX-XXX-8864, that, according to Victim D, Victim D used in or around September 2017.

40. According to search warrant returns, on or about September 19, 2017, gregmoore2424@gmail.com sent an email to Victim D's email address containing the

[1] These messages, which had been deleted, were partially recovered during the forensic analysis of ETA's Phones.

mystery shopper letter. In summary, the letter instructed Victim D to deposit two checks s/he received with the letter, perform the mystery shopper duties, and then wire the remaining funds to Individual S.C. via Western Union.

41. Furthermore, based on a review of ETA Phone 2, information regarding a money transfer appeared in an BBM communication dated on or about September 22, 2017, listing the name of Victim D, with the number XXXX7507. According to bank records, Victim D is the account holder for account XXXX7507.

42. Additionally, on or about September 22, 2017, Victim D's name appeared in further communications on ETA's Phones stating the following: "[XXXX]7507 [Victim D]" with a state and zip code corresponding to Victim's D's residence. These messages on ETA's Phones further indicate that ETA was involved in or had knowledge of the scheme to defraud Victim D.

43. Based on search warrant returns, on or about September 22, 2017, Victim D sent an email to gregmoore2424@gmail.com stating:

> I am grateful for your connection and I have completed my mission with in 24 hrs. I have copies of the receipts and of my mission. I would like to know what is convenient for you to receive my professional progress[.]

44. Based on a search of ETA Phone 1, several TextMeUp messages were recovered from ETA Phone 1 that occurred on or about September 22, 23, and 28, 2017, between "Greg Moore," using user ID "greenmoore558101," and Victim D, using telephone number XXX-XXX-8864, as follows:

Victim D:	If the proper material is not sufficient please let me know and I will make sure that I will resend it. I just need to know what you have and what you need to make sure that I have

	done my job that you sent me Please let me know if I missed anything.
"greenmoore558101":	Hello good morning [Victim D].
Victim D:	Good morning
"greenmoore558101":	How are you doing today
Victim D:	I sent in my report to Evaluationreports2@earthlink.net
"greenmoore558101":	Did you get the rest balance sent yet
Victim D:	I am going to check today I got a unusual answer on the phone that the other check may take 1 week to clear the check for [$]995.00 I would got to the bank but the other check wasn't certified check the one for [$]1974.00 Report was well written for all the assignment was for
"greenmoore558101":	The one for [$]995.00
* * *	
Victim D:	I am grateful for your connection and and what you did. I would like to tell you that you fucked the wrong person . . .

45. On or about October 15, 2018, law enforcement interviewed Victim D. Victim D stated, in summary, that s/he had been victimized by the individual operating the gregmoore2424@gmail.com account with a loss of approximately $2,969, which is what Victim D meant in the last message above (". . . you fucked the wrong person . . .). As instructed in the mystery shopper letter, Victim D deposited the checks into Victim D's bank account. Victim D then withdrew cash, performed

his/her mystery shopper duties, and then wired the remaining funds in the approximate amounts of $1,974 and $995 to Individual S.C. via Western Union.

46. According to Victim D and Victim D's bank records, on or about September 26, 2017, shortly after Victim D sent the funds as instructed, Victim D was notified by his/her bank that the checks Victim D had just deposited into Victim D's Bank of America account XXXXX3206 had been returned as fraudulent. Victim D's bank notified Victim D that s/he was responsible for paying the bank for the lost funds. Victim D reported that s/he ultimately lost at least $1,700 in the scheme.

5. Mystery Shopper Scam of Victim E

47. According to search warrant returns, on or about January 22, 2017, gregmoore2524@gmail.com, sent an email to Victim E at Victim E's email address containing a mystery shopper letter. The mystery shopper letter was purportedly sent by "[Individual C.J.]," "Survey/Evaluation Analyst" who endorsed the letter and provided his/her email address, and a text-only number. The letter informed Victim E that a "packet" should be received, presumably with a check, for his/her first secret shopper assignment. Victim E was instructed to deposit the check in his/her bank account, withdraw the cash, evaluate the employees and facilities of two different MoneyGram facilities, and send the balance of the funds minus a commission to Individual L.P. in Texas, and Individual T.S. in Illinois. Victim E was encouraged to complete his/her assignment as soon as possible and receive an extra $500 MoneyGram gift voucher. The letter stated Victim E should not divulge s/he is a

secret shopper. S/he was further instructed to send his/her evaluation report to Individual C.J.'s email address.

48. According to search warrant returns, on or about January 23, 2018, Victim E sent an email to gregmoore2524@gmail.com confirming s/he deposited the check sent for performing his/her mystery shopper duties. An email reply was sent from gregmoore2524@gmail.com back to Victim E giving Victim E further instructions and requesting a phone number for texting. Victim E replied with his/her telephone number.

49. On or about October 11, 2018, Victim E was interviewed by law enforcement regarding his/her employment as a Mystery Shopper for Individual C.J. Victim E stated s/he accepted employment with Individual C.J after receiving the mystery shopper letter. Victim E confirmed receiving the check in the mail and completing the mystery shopper duties as instructed. Victim E also confirmed that telephone number sent back to gregmoore2524@gmail.com was his/her telephone number in January 2018. Victim E reported a loss of approximately $989.

6. Mystery Shopper Scam of Victim F

50. According to search warrant returns, on or about May 17, 2017, greenmoore55@gmail.com, sent an email to Victim F at Victim F's email address containing a mystery shopper letter. The mystery shopper letter was purportedly sent by the "Evaluation team," providing email addresses greenmoore55@gmail.com and surveyreport@post.com for contact information. The letter informed Victim F that payment would be sent for his/her mystery shopper duties. Victim F was instructed

to cash the received money order at Victim F's bank and proceed with the specified task. Victim F's instructions included purchasing $20 worth of personal items and then evaluating Money Gram money transfer services. Victim F's commission was to be $150, the balance of money left after sending a money transfer for $805, minus transfer fees, to Individual R.S. in Chicago, Illinois 60613. The letter also stated Victim F should not divulge s/he is a survey/research agent.

51. On or about November 28, 2018, law enforcement interviewed Victim F. In summary, Victim F stated that on or about May 19, 2017, s/he initiated his/her mystery shopper duties, by depositing a $975 check received in the mail with the mystery shopper letter into his/her Chase Bank account XXXXXX8067. Victim F then purchased approximately $20 worth of personal items and then sent a Money Gram money transfer of $793.25 to Individual R.S. Victim F completed his/her duties by emailing surveyreport@post.com with his/her evaluation results, the Money Gram money transfer reference number, and the amount of the transfer.

52. According to Victim F, and Victim F's bank records, on or about May 22, 2017, Victim F received notice from Chase Bank that the check s/he deposited in to his/her Chase Bank Account was altered/fictitious and had been returned. Victim F lost approximately $987 as a result of his/her involvement in the scheme because s/he was responsible for reimbursing his/her bank that amount.

53. According to MoneyGram records, on or about May 19, 2017, Victim F submitted a MoneyGram wire transfer in the amount of approximately $793.25 to Individual R.S.

B. OLANIYI ADELEYE OGUNGBAIYE and Co-conspirator L.M.

54. As explained more below, further analysis of ETA's Phones, pursuant to search warrants, revealed communications involving fraudulent activities between OGUNGBAIYE and ETA. In coordination with ETA, OGUNGBAIYE received illicitly-obtained monies from these scams and was directed by ETA to transfer these funds to co-conspirators in Nigeria.

55. Specifically, search warrant returns revealed BBM and Skype communications on ETA's Phones between ETA and OGUNGBAIYE revealed several messages from approximately July 2017 to approximately February 2018 directing the transfer of money from United States bank accounts to numerous bank accounts in Nigeria, owned by co-conspirators.

56. According to search warrant returns, on or about November 15, 2017, ETA and OGUNGBAIYE communicated about the specific language to be used in response to a mystery shopper scam victim, as follows:

OGUNGBAIYE:	Your second assignment would be a bit different, go to walmart and use your debit card to send the money gram part of your assignment to the same information you did the first assignment to okay
OGUNGBAIYE:	Correct?
ETA:	yea

57. As explained below, in addition to these conversations, a review of ETA's Phones revealed that ETA and co-conspirators shared access information for several email accounts. These communications included email account addresses followed by

passwords, for accounts that were later used to commit cyber-enabled fraud scams, such as mystery shopper scams.

58. For example, the search of ETA Phone 2 revealed the following communication from on or about October 25, 2017, involving the email account greenmoore55@gmail.com, which I believe to be an account used and controlled by ETA, as described in the scam of Victim F (section III.A.6 above):

ETA:	mailto: greenmoore55@gmail.com
ETA:	Pencil123456 [possible password for greenmoore55@gmail.com]
OGUNGBAIYE:	na d login for the textmeup b dis abi [Is this the login for the textmeup application?][2]
ETA:	Yea [Yes]

59. Another example of co-conspirators sharing email address information were included in BBM communications on or about September 6, 2017, obtained from the execution of a search warrant of ETA Phone 2, regarding email accounts Olaniyiogungbaiye@gmail.com and olaniyiogungbaiye@yahoo.com:

ETA:	Give me d email u one dey use talk to d gal [Give me the email address that you want to use to talk to the woman]
OGUNGBAIYE:	Mke i use my olaniyiogungbaiye@yahoo.com [Should I use olaniyiogungbaiye@yahoo.com?]
OGUNGBAIYE:	Or mke i open new email [Or should I create a new email address?]

[2] The bracketed statements are based on a draft translation by law enforcement personnel familiar with linguists in the Yoruba language, combined with my training and experience in this and other investigations. This translation is not to be treated as final official translations or interpretations.

OGUNGBAIYE: Olaniyiogungbaiye@gmail.com

ETA: OK

1. Email Harvesting

60. In order to execute large schemes, a substantial victim base must be obtained. Harvesting email addresses of victims allowed ETA and his co-conspirators the ability to target thousands of victims all over the world. Based on my training and experience, one way to harvest email addresses is through an email harvesting tool, which extracts large numbers of email addresses from various sources including websites or search engines. Based on my training and experience, criminals can then use these emails to conduct fraudulent activities such as mystery shopper scams, romance scams, business email compromise scams or to conduct malicious phishing activities to collect unsuspecting victim usernames and passwords.

61. During the investigation, it was discovered that two email harvesting tools were sent to OGUNGBAIYE for use in the various fraud schemes. A review of OGUNGBAIYE's email account found that he was sent one email extractor tool by ETA and one by Co-conspirator L.M. OGUNGBAIYE's email account also showed a collection of emails containing links that appeared to be malicious in nature. Further review of the emails revealed that many of the links served the purpose of collecting users' login credentials. For instance, in one email, if an unsuspecting victim clicked the link in the malicious email, they would be redirected to a webpage displaying a textbox asking for account verification information, otherwise their account would be shutdown.

62. Based on search warrant returns, these email harvesting tools enabled OGUNGBAIYE and Co-conspirator L.M. to create mailing lists for mystery shopper solicitations. These types of mailing lists were shared between co-conspirators and with individuals preparing the counterfeit USPS money orders and counterfeit checks to be mailed to prospective victims throughout the United States. Similar lists were found in ETA's many email accounts which included the following: greenmoore55@gmail.com, gregmoore2424@gmail.com, gregmoore2524@gmail.com and robbybabe1@yahoo.com.

63. According to search warrant returns, numerous emails were exchanged between gregmoore2424@gmail.com, greenmoore55@gmail.com and gregmoore2524@gmail.com, all using the name "Greg Moore" (or a variation thereof), indicating that ETA's use of these email addresses are likely connected.

64. Additionally, a search warrant return of OGUNGBAIYE's email account, donchichivirus@gmail.com, revealed over 300 attempts, mostly successful, to gather username and password combinations from victims and at least two attempts of gathering bank account information from victims. The usernames and password combinations were either delivered directly to OGUNGBAIYE's email account from what appeared to be a server address, or forwarded to OGUNGBAIYE's email account from an unknown individual.

65. A search of another of OGUNGBAIYE's email accounts, olaniyiogungbaiye@yahoo.com, revealed that on or about July 11, 2016, OGUNGBAIYE was advised by Co-conspirator L.M., using a yahoo.com email

address, on how to best use the email extractor tool by using long string searches in order to filter the type of email addresses they wanted to collect. Co-conspirator L.M., him/herself, had an email account that holds over 700 instances of business email compromise as well as over 400 usernames and passwords combinations or attempts at gaining username and password combinations. Additionally, according to search warrant returns, Co-conspirator L.M.'s yahoo.com account also attempted to collect credit card information from at least fifty victims. One business email compromise was found in both OGUNGBAIYE and Co-conspirator L.M.'s email accounts, as described below.

2. Business Email Compromise of Victim G

66. A review of search warrant data for OGUNGBAIYE's email account, donchichivirus@gmail.com, revealed that on or about November 13, 2017, OGUNGBAIYE's email account contained a message from an unknown sender that included a business email address and password credentials for Victim G, an employee of Company G. Additionally, an email dated November 27, 2017, revealed an email conversation between Victim G and Victim H, an employee of Company H. The email conversation dated back to on or about November 16, 2017, and pertained to invoicing between Company H and Company G. Specifically, Victim H sent Victim G an invoice requesting payment for $6,215.53 from Victim G.

67. According to search warrant returns, on or about November, 17, 2017, Victim H sent another email to Victim G stating that the payment can no longer be received via check and should be paid via wire transfer.

68. Based on search warrant returns, on or about November 22, 2017, Victim G responded to Victim H's email stating Company G would make the payment on November 27, 2017. Additionally, the response appeared to be sent to the legitimate email address of Victim H because the displayed name and email address of the message read as the legitimate email address of Victim H. However, the actual email address that the displayed name and email address linked to was in fact one of Co-conspirator L.M.'s yahoo.com email addresses.

69. Based on search warrant returns, on or about November 27, 2017, Victim G emailed Victim H, which was routed to Co-conspirator L.M.'s yahoo.com email address, stating that Victim G had been trying to call Victim H with the number on Victim H's last email and website but a response of "number not in use" message played. The email also stated that a wire for $2,158.21 was made on this day from Company G as previously directed.

70. According to search warrant returns, later on or about November 27, 2017, Victim H's email address responded to Victim G stating, "So sorry we are out of phone at the moment," and instructed that Victim G actually owed $6,215.53 and Company G should pay $4,100 as soon as possible. The same day, the Victim G stated that Company G sent $4,100 via wire transfer.

71. According to bank records, Victim G wired the funds not to Company H, but rather to a bank account owned by an individual named "Marcus Smith."

72. Based on the actions above and my training and experience, I believe that OGUNGBAIYE harvested the credentials of Victim G and shared them with Co-

conspirator L.M. in order to steal funds from Company G. I believe that Co-conspirator L.M. used Victim G's credentials to surveil Victim G's email account until an opportunity, such as invoicing, arose. Once an opportunity arose, Co-conspirator L.M. interjected him/herself into a conversation between Victim G and Victim H, told Victim G to wire funds to a fraudulent account, and routed all further conversations that were intended for Victim H, to Co-conspirator L.M.'s yahoo.com email address. Further, according to search warrant returns, Co-conspirator L.M. would send all outbound emails to Victim G from an email address that was identical to Victim H, but all return emails from Victim G to that address were directed to Co-conspirator L.M.'s yahoo.com email address.

73. On or about October 31, 2017, bank surveillance footage showed a man later identified by CS-1 as co-conspirator IDOWU depositing funds into the aforementioned bank account of "Marcus Smith."

74. A message containing bank account information in the name of "Marcus Smith" was observed on ETA Phone 2 dated on or about November 24, 2017, indicating that ETA had knowledge of this account and the overall scheme.

C. BABABTUNDE LADEHINDE LABIYI

75. A review of ETA's Phones revealed an image of a fraudulent French passport, number XXXXX5964, in the name of "Chattman Ronald Stewart" as well as an image of a fraudulent United Kingdom passport, number XXXX4629, in the name of "Beckham Smith Dave." These two passports contained an identical photograph in two different names. Additionally, ETA Phone 1 contained a copy of the original

image of the photograph that the aforementioned passport thumbnail photos were derived from, indicating that ETA had knowledge of this photograph.

76. According the French government, the above-referenced French passport in the name of "Chattman Ronald Stewart" is fraudulent.

77. According to the British government, the above-referenced United Kingdom passport in the name of "Beckham Smith Dave" is fraudulent.

78. In the course of investigating the true identity of "Chattman Ronald Stewart," law enforcement reviewed the Illinois driver's license photograph of LABIYI provided by the Illinois Secretary of State.

79. According to the FBI's Forensic, Audio, Video and Image Analysis Unit, the photograph from the passport in the name of "Chattman Ronald Stewart" appears to be the same individual as the Illinois driver's license photograph of LABIYI based on "multiple similar characteristics and several unique characteristics."

80. On or about June 18, 2018, CS-1 identified the passport photograph of "Chattman Ronald Stewart" and "Beckham Smith Dave" by the alias "Junior," stating that "he works for ETA" and that "Junior" gives ETA cash and money orders that CS-1 believed to originate from fraudulent activity.

81. Having reviewed the aforementioned photographs, and based on my experience in this investigation, I believe the passport photograph of "Chattman Ronald Stewart" and "Beckham Smith Dave" and LABIYI's Illinois driver's license photograph appear to be the same person.

82. These two passports were used to open approximately fourteen U.S. bank accounts in the aforementioned fraudulent names of "Chattman Ronald Stewart" and "Beckham Smith Dave" (or variations thereof), as indicated both in bank records and referenced in messages obtained from ETA's Phones.

83. Several of these bank accounts included the email addresses chattmanstewart@gmail.com or bechamdave@gmail.com in the account opening documents. A review of search warrants records for these email addresses further linked these fictitious names to LABIYI.

84. For instance, email records indicated that email address bechamdave@gmail.com was linked by cookies to the email addresses labiyi@gmail.com, labiyi500@gmail.com and chattmanstewart@gmail.com.[3] Email account labiyi@gmail.com was registered to "Junior Labiyi" with phone number XXX-XXX-0006.

85. Telephone subscriber records indicate phone number XXX-XXX-0006 is assigned to LABIYI.

86. According to court authorized pen register trap and trace data, from approximately April 25, 2017, to on or about September 16, 2018, phone number XXX-XXX-0006 has communicated at least 631 times with ETA by text message or voice calls.

[3] Google keeps records that can reveal accounts accessed from the same electronic device, such as the same computer or mobile phone, including accounts that are linked by "cookies," which are small pieces of text sent to the user's Internet browser when visiting websites.

87. On or about May 30, 2018, records from Blackberry Corporation indicated that BBM PIN XXXXF4E7 was associated with phone number XXX-XXX-0006.

88. According to a second court authorized pen register trap and trace data regarding BBM PIN XXXXF4E7, from on or about November 2, 2017, to on or about April 10, 2018, LABIYI, communicated at least 106 times with ETA.

89. Information recovered from ETA's Phones included that from approximately May 2017 to approximately February 2018, the fictitious name "Chattman Ronald Stewart" (or a variation thereof) with multiple bank account numbers appear at least 34 times in the form of text messages, BBM messages and/or Skype messages. Also, from approximately May 2017 to approximately February 2018, the fictitious name "Beckham Dave Smith" (or a variation thereof) with multiple bank account numbers appears at least 19 times in the form of text messages, BBM messages and/or Skype messages. These communications indicate that ETA was not only knowledgeable about the accounts in these fictitious names, but communicated them to various known and unknown co-conspirators in furtherance of this wire fraud scheme, including OGUNGBAIYE.

1. Romance Scam of Victim I

90. ETA's Phones also contained evidence of multiple romance scams in which ETA conspired with LABIYI to obtain victim money derived from online fraud. For example, contained within ETA's Phones was a screenshot displaying a bank

transaction receipt for a $33,000 wire transfer from Victim I's TD Bank account to Citi Bank account number XXXXX7106 registered to "Chattman Ronald Stewart."

91. According to records obtained from Citibank, on or about January 24, 2018, account XXXX7106 registered to "Chattman Ronald Stewart" received a $33,000 wire transfer from Victim I.

92. In July and August 2018, Victim I was interviewed by law enforcement and confirmed s/he made the $33,000 wire transfer. Victim I provided law enforcement with his/her bank records indicating the $33,000 wire transfer on or about January 24, 2018, that Victim I made from his/her TD Bank account number XXXXXX6012 to the "Chattman Ronald Stewart" account listed above. Victim I's bank records further indicate the $33,000 was wired immediately following a deposit into Victim I's account of $35,393.50. As a result, Victim I was an unwitting money mule in this scheme. Victim I stated, in summary, that s/he met an individual by the name of "Ed Gunn" online through Facebook in response to Victim I's Facebook post regarding relationship difficulties. In approximately November 2016, "Ed Gunn" introduced Victim I to an individual by the name of "Suave Rochet," a resident of Nigeria. Victim I communicated via text messaging with "Suave Rochet" two to three times daily and referred to him/her as his/her boy/girlfriend. "Suave Rochet" transferred in excess of the $33,000 Victim I transferred in multiple increments into Victim I's bank account from approximately June 2017 to May 2018. "Suave Rochet" claimed the money was from an inheritance and recruited Victim I through the romance scam to launder the money for "Suave Rochet."

2. Romance Scam of Victim J

93. In another example, both of ETA's Phones contained a screenshot dated on or about October 15, 2017. That screenshot displayed a Chase Bank transaction receipt for a $3,000 wire transfer from Victim J's JPMorgan Chase Bank account to Citi Bank account number XXXXX7106 registered to "Chattman Ronald Stewart."

94. On or about January 26, 2018, Victim J called the FBI public access line to report a romance scam and a purported loss of approximately $105,000. Victim J stated s/he met an individual online, "Emilia Alois." Victim J stated that on or about October 14, 2017, s/he wired approximately $3,000 to Citibank account number XXXXX7106, to "Chattman Ronald Stewart."[4]

95. On or about August 9, 2018, Victim J was interviewed by law enforcement. Victim J stated that s/he met "Emilia Alois" on Match.com.[5] "Emilia Alois" indicated that she was from West Hollywood, California, and told Victim J that she needed to go to Brazil to compete for a road project. Upon returning to West Hollywood, "Emilia Alois" told Victim J that she had won the project but needed to pay a $3,000 fee to get the equipment out of port and onto the job site. Victim J confirmed that on or about October 14, 2017, s/he sent $3,000 from his/her JPMorgan Chase Bank account to a "friend" of "Emilia Alois" (as described above).

[4] Victim J also wired additional funds to individuals not named in this complaint.

[5] The "Emilia Alois" account has since been suspended by Match.com.

3. Romance Scam of Victim K

96. In a third example, in or around October and November 2018, Victim K was interviewed by law enforcement. Victim K stated, in summary, that on or about September 2017, s/he was contacted unexpectedly on Instagram by a woman identified as "Sarah Allison." "Sarah Allison" advised that she was looking for a friend and Victim K began communicating with her via Instagram on a daily basis. "Sarah Allison" explained that she had lived in New York, Texas, and now resided in London, England. In or around November 2017, "Sarah Allison" informed Victim K that she was in receipt of a $2.5 million inheritance, but she needed financial help to have the money released. Victim K agreed to help. To assist with Victim K's payments, "Sarah Allison" used Instagram to introduce Victim K to an attorney in Rome, Georgia, identified as "Ronald Bennetti, Sr." According to "Ronald Bennetti, Sr.'s" instructions, Victim K used his/her own money to deposit funds into accounts at Fifth Third Bank, JPMorgan Chase Bank, and Bank of America. Victim K also stated that s/he communicated with several other online individuals regarding this matter as introduced by "Sarah Allison" and/or "Ronald Bennetti, Sr."

97. Victim K stated to law enforcement that s/he recalled the names "Beckham Smith Dave" and "Chattman Ronald Stewart" and stated that s/he sent money to bank accounts owned by these individuals. Victim K provided a list of individuals that s/he communicated with and to whom s/he sent money, which included the aforementioned names as well as "Samuel C. Giles" (as discussed below with respect to ANIFOWOSHE) and "Charles Mark" (as discussed below with respect

to AKARIGIDI). Victim K then provided receipts of money transfers s/he made from approximately November 2017 to approximately October 2018 on behalf of the aforementioned online personas. Victim K provided two bank receipts to law enforcement in which Victim K used his/her own funds to deposit money as a result of the romance scam: (1) on or about December 6, 2017, for a $20,000 cash deposit from Victim K into a Fifth Third checking account ending in XXXXXX6802; and (2) on or about December 15, 2017, for a $3,100 cash deposit from Victim K into the same Fifth Third checking account ending in XXXXXX6802.

98. Records obtained from Fifth Third Bank account XXXXXX6802 registered to "Beckham Smith Dave" indicated that on or about December 6, 2017, and December 15, 2017, two cash transactions were deposited in the amounts of $20,000 and $3,100, respectively.

99. Additionally, Victim K provided law enforcement with a receipt for a wire transfer on or about December 28, 2017, for $15,000 from Victim K's bank account to Citibank account number XXXXX7106 in the name of "Chapman Ronald Stewart."[6]

100. According to Citibank bank records, account XXXXX7106 was registered to "Chattman Ronald Stewart" and received a $15,000 wire transfer on or about December 28, 2017, from Victim K.

[6] I believe this is a typographical error either by Victim K or the bank employee who processed the transaction.

4. Romance Scam of Victim L

101. In a fourth example, on or about October 25, 2018, Victim L was interviewed by law enforcement about romance scams, namely about "Chattman Ronald Stewart" and "Samuel Giles" (discussed below in section III.E.2). Victim L showed law enforcement personal notes with the name "Chattman Ronald Stewart," with bank account number XXXXX7106, previously linked to a Citibank account, as well as other receipts showing multiple wire transactions going to various individuals. Citibank account records indicate that the account XXXXX7106 held in the fictitious name of "Chattman Ronald Stewart," matches the account number written in Victim L's personal notes. Citibank account records for account XXXXX7106, in the name of "Chattman Ronald Stewart," reflect a $17,266.83 wire transfer from Victim L on or about April 2, 2018. According to Victim L, due to this fraud scheme, s/he suffered an estimated financial loss of approximately $75,000, which was secured by taking out a personal loan.

102. On approximately nine previous occasions, Citibank account number XXXXX7106 with the corresponding name "Chattman Ronald Stewart" (or a variation thereof) appeared in ETA's phone communications to unknown co-conspirators, indicating ETA was aware of this fictitious name and account number. Based on my training and experience, numerous transactions from one victim (Victims L and K, for example) to multiple co-conspirators in this investigation further corroborate the overall conspiracy.

D. BARNABAS OGHENERUKEVWE EDJIEH

103. A review of ETA's Phones revealed an image of a fraudulent United Kingdom passport number XXXXX8905 in the name of "Garry Jimmie Stephen."

104. According to information obtained from the British government, the above-referenced United Kingdom passport in the name of "Garry Jimmie Stephen" is fraudulent.

105. In the course of investigating the true identity of "Garry Jimmie Stephen," law enforcement obtained an Illinois driver's license of EDJIEH. Based on my experience in this investigation, the photograph of EDJIEH appears to be the same individual in the passport photograph of "Garry Jimmie Stephen."

106. According to the FBI's Forensic, Audio, Video and Image Analysis Unit, the photograph submitted from the passport in the name of "Garry Jimmie Stephen" appears to be the same individual as the Illinois driver's license photograph of EDJIEH based on "multiple similar class characteristics and several unique characteristics."

107. On or about June 18, 2018, CS-1 identified the passport photo of "Garry Jimmie Stephen" as a person CS-1 knew as "Barnabus" from observing him on occasion meeting in person with ETA.

108. This passport was used to open three U.S. bank accounts in the aforementioned fraudulent name of "Garry Jimmie Stephen" (or a variation thereof), as indicated both in bank records and referenced in messages obtained from ETA's Phones, and discussed below in the romance scam of Victim M.

109. All three of these bank accounts included the email address coreykiddwittstock@gmail.com in the account opening documents. A review of search warrant records for this email address further linked this fictitious name to EDJIEH. For instance, email records indicated that this email address was linked by cookies to the email addresses edjiehbarnabas@gmail.com and edjiehjudith@gmail.com. Email account edjiehbarnabas@gmail.com was registered to "Barnabas Edjieh" with phone number XXX-XXX-6461. Email account edjiehjudith@gmail.com was registered to "Edjieh Judith."

110. According to court authorized pen register trap and trace data from on or about April 6, 2017, to on or about September 12, 2018, phone number XXX-XXX-6461, registered to EDJIEH communicated at least 590 times with ETA by text message or voice call.

111. A law enforcement database search for phone number XXX-XXX-6461 resolved to a "Barnabas Edjieh" with an associated address in Chicago, Illinois.

112. A review of the search warrant internet search history of coreykiddwittstock@gmail.com revealed that from on or about January 30, 2017, to on or about April 26, 2018, driving directions to the same address in Chicago, Illinois, mentioned immediately above, was searched over 600 times.

113. Additionally, from on or about March 8, 2017, to on or about April 15, 2018, driving directions to a specific address in Chicago, Illinois 60645 was searched over 50 times. According to CS-1, this specific address is where CS-1 observed EDJIEH meet ETA.

114. Additional information gathered from ETA's Phones revealed that from approximately May 2017 to February 2018, the fictitious name "Garry Jimmie Stephen" (or a variation thereof) with multiple bank account numbers appears at least eight times in the form of a text, BBM, and/or Skype message. These communications indicate the ETA was not only knowledgeable about the accounts in these fictitious names, but communicated them to various co-conspirators in furtherance of this wire fraud scheme.

1. Romance Scam of Victim M

115. Based on search warrant returns for ETA Phone 2, on or about September 18, 2017, ETA sent a BBM message to another BBM account that he controlled containing Bank of America account number XXXXXXXX3320, the title of the account as "Garry J Stephen," and routing number XXXXX4808.

116. According to records obtained from Bank of America, account XXXXXXXX3320 was registered to "Garry Jimmie Stephen" and received a $13,000 cash deposit on the same day as the aforementioned BBM message.

117. On or about September 26, 2018, Victim M was interviewed by law enforcement. Victim M stated, in summary, that s/he has been communicating online with an individual named "Dave King" since approximately December 2016. Victim M first met "Dave King" through the online dating service. "Dave King's" profile indicated "Dave King" was from the Kokomo, Indiana area. Victim M and "Dave King" communicated three or four times a week, primarily through text messaging but also on the phone.

118. According to Victim M, s/he accepted and transferred money on behalf of and at the direction of "Dave King" approximately 20 times since their relationship began, consistent with the activities of an unwitting money mule. Victim M used both Western Union and Money Gram to send "Dave King" money in increments varying from $700 to $10,000. Victim M confirmed that s/he had sent $13,000 on behalf of "Dave King" in or around September 2017. In this instance, monies were sent to Bank of America account XXXXXXXX3320 because Victim M was not able to use Western Union or Money Gram for that particular transaction. Victim M stated that s/he has not kept any of the money sent to him/her from "Dave King," and in fact has sent "Dave King" approximately $6,000 to $7,000 of his/her own money.

E. SULTAN OMOGBADEBO ANIFOWOSHE

119. A review of ETA's Phones revealed that from approximately October 2017 to approximately February 2018, the fictitious name "Samuel Christopher Giles" (or a variation thereof) with an associated bank account number appears at least 15 times in the form of a text, BBM and/or Skype message, including on at least one occasion to OGUNGBAIYE, consistent with the wire fraud schemes described above.

120. In the course of investigating the true identity of "Samuel Christopher Giles," law enforcement obtained an Illinois State identification photograph of ANIFOWOSHE.

121. On or about June 18, 2018, CS-1 identified the Illinois State identification photograph of ANIFOWOSHE by the name "Ayinde," and stated that

ANIFOWOSHE works with ETA to cash out money orders that CS-1 has observed ETA tell ANIFOWOSHE to go pick up.

122. Law enforcement has reviewed Fifth Third bank records and still images of video footage pertaining to an account opened in the name of "Samuel Christopher Giles." These documents included a scanned copy of a United Kingdom passport XXXXX9368 in the name of "Samuel Christopher Giles" as well as two images of an individual inside a Fifth Third branch location. The first photo, dated November 13, 2017, at 3:59:08 p.m. Central Standard Time (CST), shows this individual at the teller station when the account was opened. The second photo, dated November 16, 2017, at 11:00:23 a.m. CST, shows what appears to be the same individual at the teller station withdrawing $9,000.

123. According to information obtained from the British government, the United Kingdom passport XXXXX9368 in the name of "Samuel Christopher Giles" is fraudulent.

124. On or about July 27, 2018, CS-1 was shown the aforementioned United Kingdom passport photograph in the name of "Samuel Christopher Giles" and the two Fifth Third Bank branch teller photographs. CS-1 identified the passport photograph of "Samuel Christopher Giles" by the name "Ayinde," which was previously associated to the Illinois state identification photograph of ANIFOWOSHE.

125. Based on my experience in this investigation, I believe that the United Kingdom passport photograph of "Samuel Christopher Giles," appears to be ANIFOWOSHE as depicted in his Illinois state identification photograph.

126. According to bank records and information obtained from bank investigators, United Kingdom Passport XXXXX9368 was used to open five U.S. bank accounts in the name "Samuel Christopher Giles" (or a variation thereof), each time utilizing s.giles439@outlook.com as the email address associated with this fictitious identity.

127. Search warrant records obtained for email account s.giles439@outlook.com identified three emails from Bank of America indicating that debit cards were sent to "SAMUEL C GILES" at an address in Chicago, Illinois.

128. A search through a law enforcement database has ANIFOWOSHE associated with the aforementioned address. Additionally, the United States Postal Service reports mail in the name of ANIFOWOSHE has been delivered to the same aforementioned address.

1. Romance Scam of Victim K

129. In furtherance of this wire fraud scheme, Victim K, previously discussed as an online victim as it pertained to co-conspirator LABIYI (*infra* at section III.C.3), and will be discussed in relation to AKARIGIDI (*supra* at section III.F.1), also transferred money to ANIFOWOSHE under the false pretenses of a romance/inheritance scam at the direction of the lawyer "Ronald Bennetti Sr." Specifically, a money transaction receipt provided to law enforcement by Victim K

indicated a $1,500 wire transfer from Victim K's JPMorgan Chase bank account on or about April 12, 2018, to Byline Bank account number XXXXXX1270 in the name of "Samuel Christopher Giles." Victim K confirmed to law enforcement that s/he sent the $1,500 to account XXXXXX1270, as instructed by "Ronald Bennetti, Sr."

130. According to Byline Bank records, account XXXXXX1270 registered to "Samuel Christopher Giles" received a $1,500 wire transfer on or about April 12, 2018, from Victim K. Numerous transactions from one victim, Victim K, to multiple co-conspirators show these defendants are part of the same conspiracy.

2. Romance Scam of Victim L

131. On or about October 25, 2018, Victim L was interviewed by law enforcement. Victim L stated, in summary, that s/he met "Yussif Ibrahim," who uses the name "Frank," online through Facebook in response to Ibrahim's Facebook friend request. Victim L, who told law enforcement that s/he was a recent widow/er, accepted the friend request out of loneliness. Victim L and "Frank" engaged in a romantic relationship online via Facebook, email and Google Hangout. Assurances by "Frank" that "Frank" would join Victim L in the United States for a future together led Victim L to send money to "Frank" and his friends to help "Frank" pay for his son, "Sam's" medical bills. Victim L sent money via Western Union and bank wire transfers to multiple individuals, including "Samuel Christopher Giles" and "Chattman Ronald Stewart."

132. According to Victim L, on or about November 21, 2017, and on or about December 13, 2017, Victim L deposited personal funds in the forms of a $13,700

cashier's check and a $14,220 cashier's check, respectively, in to PNC Bank account XXXXXX4801 in the name of "Samuel Giles." Victim L maintained personal notes and receipts with "Samuel Giles's" PNC Bank account number XXXXXX4801 and bank address in Chicago. PNC Bank account records for the account held in the fictitious name of "Samuel Giles" reflects both deposits.

F. BABATUNDE IBRAHEEM AKARIGIDI

133. A review of ETA's Phones revealed that from approximately July 2017 to approximately February 2018, the fictitious name "Charles Mark" (or a variation thereof) with an associated bank account number appears at least four times in the form of a text, BBM and/or Skype message, consistent with the scheme to defraud.

134. In the course of investigating the true identity of "Charles Mark," law enforcement obtained an Illinois driver's license photograph of AKIRIGIDI.

135. On or about June 18, 2018, CS-1 identified the Illinois driver's license photograph of AKARIGIDI by the name "AK," stating that "AK" was likely involved in fraudulent activities with ETA and that CS-1 observed AK ask ETA for bank information to do money transfers.

136. Bank account opening records include a scanned copy of a United Kingdom Passport XXXXX8493 in the name of Charles Mark. The bank also provided two images of an individual inside a branch location dated December 5, 2017, at 12:52:49 p.m. CST and December 5, 2017, at 1:39:53 p.m. CST, which show this individual at the teller station when the account was opened.

137. According to information obtained from the British government, the above-referenced United Kingdom passport in the name of "Charles Mark" is fraudulent.

138. On or about July 27, 2018, CS-1 identified the passport photograph of "Charles Mark" and the two aforementioned bank teller images as the person CS-1 knew by the name "AK," which was previously identified as the Illinois driver's license photograph of AKARIGIDI. CS-1 further stated that CS-1 has seen "AK" several times with ETA.

139. Based on my experience in this investigation, I believe that the passport photograph of "Charles Mark" appears to be AKARIGIDI.

140. According to bank records and officials, United Kingdom Passport XXXXX8493 in the name of "Charles Mark" was used to open four U.S. bank accounts in the name "Charles Mark" (or a variation thereof), each time utilizing markcharles0484@gmail.com as the email address associated with this fictitious identity.

141. Search warrants records obtained for email account markcharles0484@gmail.com revealed additional information linking the fictitious name "Charles Mark" to AKARIGIDI. For instance, email records indicated that email address markcharles0484@gmail.com was linked by cookies to the email addresses bakarigidi@gmail.com and ibraheema7919@gmail.com. Email address bakarigidi@gmail.com was registered to "B A." Email address ibraheema7919@gmail.com was registered to "ibraheema a."

1. Romance Scam of Victim K

142. In furtherance of this wire fraud scheme, Victim K, previously discussed as an online victim as it pertained to co-conspirators LABIYI and ANIFOWOSHE, also transferred money to AKARIGIDI under the false pretenses of a romance/inheritance scam at the direction of the lawyer "Ronald Bennetti Sr." Specifically, a money transaction receipt provided to law enforcement by Victim K indicated a $15,000 cash deposit from Victim K on or about January 4, 2018, to Fifth Third Bank account number XXXXXX9699 in the name of "Charles Mark."

143. According to Fifth Third Bank records, account XXXXXX9699 registered to "Charles Mark" received a $15,000 deposit on or about January 4, 2018. Based on my training and experience, numerous transactions from one victim, Victim K, in particular, to multiple co-conspirators in this investigation show these individuals are part of the same conspiracy.

2. Employment Scam of Victim N

144. On or about November 28, 2018, Victim N was interviewed in person by law enforcement. In summary, Victim N stated that s/he was hired by an individual named "Jackson Walker" to work at an online company called Noblon LLC as an accounts payable clerk. Noblon LLC was purportedly located in Corpus Christi, Texas. Victim N's job was to handle payments to Noblon LLC's vendors. Victim N utilized his/her personal bank accounts at Wells Fargo Bank, JPMorgan Chase Bank and Bank of America, one of which was opened at the direction of "Jackson Walker," to make payments to vendors. Victim N received deposits into his/her bank accounts,

then withdrew the money as cash, checks or money orders and deposited the money in to various bank accounts, believing s/he was paying vendors. This scheme is consistent with the activities of an unwitting money mule.

145. Bank records obtained from JPMorgan Chase Bank account number XXXXX5625 in the name of "Charles Mark" indicated the deposit of a $28,450 Bank of America cashier's check from Victim N, on or about June 13, 2018, consistent with the aforementioned scam.

146. Furthermore, records obtained from Walmart and MoneyGram revealed that a few days later, from on or about June 14, 2018, to on or about June 18, 2018, approximately 15 money orders totaling approximately $12,800 were purchased using the $28,450 as the funding source. These money orders were purchased with debit card x0218 for JPMorgan Chase Bank account number XXXXX5625 in the name of "Charles Mark."

147. Subsequently, according to additional JPMorgan Chase records, five of these money orders were deposited into account number XXXXX2006, owned by AKARIGIDI in or around June 2018 totaling approximately $4,400. All five of these money orders had the purchaser name and recipient name written as "Babatunde Akarigidi."

148. Also, according to Bank of America records, one of these money orders was deposited into account number XXXXXX5477, owned by Insurance Auto Auctions Inc., in or around June 2018 for approximately $400.

149. Records obtained from Insurance Auto Auctions Inc., indicated that this money order was used to purchase a vehicle at auction by ETA on or about June 19, 2018. ETA provided government identification to purchase this vehicle on behalf of a Nigerian car company named Real Absolute. Based on my experience and training, this shows that ETA was a beneficiary of the fraud.

G. ADEWALE ANTHONY ADEWUMI

150. A review of ETA's Phones revealed that from approximately July 2017 to approximately February 2018, the fictitious name "Johnson Collins" (or a variation thereof) and a Bank of America account XXXXXXXX2200 (as discussed below), appears at least seven times in the form of a text, BBM and/or Skype message, consistent with the scheme to defraud.

151. According to bank records and information obtained from bank investigators, United Kingdom Passport XXXXX5243 in the name of "Johnson Collins" was used to open three U.S. bank accounts in the name "Johnson Collins" (or a variation thereof). Upon opening this account, collinsjohnson011@gmail.com and phone number XXX-XXX-8419 were recorded as the account holder's contact information.

152. According to a law enforcement database, the subscriber of phone number XXX-XXX-8419 is "Adewale Anthony Adewumi," a Nigerian national with a listed address in Texas.

153. According to telephone records, the subscriber of phone number XXX-XXX-8419 was registered to "Adewale Adewumi," address 9821 Summerwood Circle, Apt 2602, Dallas, Texas 75243 with secondary phone number of XXX-XXX-1254.

154. According to additional telephone records, phone number XXX-XXX-1254 is registered to "Adewale Adewumi" of Dallas, Texas.

155. According to court authorized pen register trap and trace data from on or about June 25, 2017, to on or about June 22, 2018, phone number XXX-XXX-1254, registered to ADEWUMI, had communicated at least 33 times with ETA by text message or voice call.

156. Email account records obtained for collinsjohnson011@gmail.com indicated that this email account was created from IP address 2602:306:bda7:a510:a133:795f:f9ae:44a4 and registered to "Collins Johnson."

157. IP address records for 2602:306:bda7:a510:a133:795f:f9ae:44a4 resolved to an individual named "Gayle Dunn" at 9821 Summerwood Circle, Apt 2602, Dallas, Texas 75243, the same address to which telephone number XXX-XXXX-1254 is registered in ADEWUMI's name.

158. Search warrant records obtained for email account collinsjohnson011@gmail.com revealed several incoming money transfers from apparent victims to a PayPal account in the name of "Johnson Collins." These deposits were then routinely transferred to a PayPal account in the name of "Adewale Adewumi," consistent with the scheme to defraud. In total, from approximately December 2017 to approximately February 2018, email activity indicated

approximately 39 money transfers sent from a PayPal account connected to collinsjohnson011@gmail.com to a PayPal account in the name of "Adewale Adewumi" totaling at least $52,000.

159. A further review of email account collinsjohnson011@gmail.com detailed approximately 10 emails in the fall of 2017 from a liberal arts university in Texas, sometimes addressed to "Adewale."

160. Records obtained from the liberal arts university in Texas indicated that an individual named "Adewale A. Adewumi" was a student at the university with the same date of birth and physical address as the driver's license information obtained from a law enforcement database search for ADEWUMI.

1. Romance Scam of Victim O

161. Bank records obtained from TCF Bank account number XXXXXX0387 opened with fictitious United Kingdom Passport XXXXX5243 in the name of "Johnson Collins" revealed a $14,999.98 check deposit from Victim O on or about November 27, 2017.

162. In or around October 2018, Victim O was interviewed by law enforcement. In summary, Victim O became an unwitting money mule in a romance scam in which an online persona by the name of "Claire Anderson" convinced Victim O that "Claire Anderson" had cancer and needed to travel to Nigeria for family reasons. Eventually, "Claire Anderson" asked Victim O for financial favors by having Victim O receive deposits into Victim O's bank accounts and turn the funds into money orders. "Claire Anderson" also had Victim O allow "Claire Anderson" to use

Victim O's accounts for the wiring in and out of large amounts of money. Victim O confirmed that s/he recalled a transaction over $14,000 taking place through one of his/her bank accounts in or around November 2017 at the direction of "Claire Anderson."

2. Romance Scam of Victim P

163. In another instance, bank records obtained for Bank of America account number XXXXXXXX2200 (as found in ETA Phone 2, above) indicate that account XXXXXXXX2200 was opened with a fictitious United Kingdom Passport XXXXX5243 in the name of "Johnson Collins." The records revealed that between on or about September 5, 2017, and on or about September 8, 2017, three transactions totaling approximately $4,800 were transferred in to this account by Victim P.

164. In or around October 2018, Victim P was interview by law enforcement. In summary, Victim P stated that s/he had been the victim of a romance scam. In or around April 2017, Victim P had signed up for a dating website where s/he had met an individual named "George Bobby Edwards," who Victim P believed to be living in Michigan. Victim P confirmed that s/he had sent a total of approximately $18,000 over a six-month period to "George Bobby Edwards" by wiring money through Walmart, Stop + Shop, and Bank of America money transfers. Victim P stated that "George Bobby Edwards" told him/her that "George Bobby Edwards" needed to pay off some debt and provided Victim P a story regarding his hard times and asked the money be made out to "Collins." "George Bobby Edwards" told Victim P that "Collins" would be paying off debt on his behalf. Victim P had the following transactions noted

in his/her check book which were made out to "Collins": September 5, 2017 - $1,000; September 7, 2017 - $1,800; and September 8, 2017 - $2,000, consistent with deposits indicated in the aforementioned Bank of America account XXXXXXXX2200.

H. MIRACLE AYOKUNLE OKUNOLA

165. A review of ETA's Phones revealed that from approximately July 2017 to approximately September 2017, the fictitious name "Luke Johnson" (or a variation thereof) with associated bank account number appears at least eight times in the form of a text, BBM and/or Skype message, consistent with the scheme to defraud.

166. In the course of investigating the true identity of "Luke Johnson" law enforcement obtained an Illinois State identification photograph of OKUNOLA.

167. In a review of publicly available information on the internet, law enforcement observed three photographs from social media accounts linked to OKUNOLA. The first photograph was an image uploaded to a Facebook account attributed to the display name "Miracle Okunola." The second and third images were uploaded to a Google account with the display name "Okunola Miracle." These images appear to be the same individual in the Illinois State identification photograph of OKUNOLA.

168. According to the FBI's Forensic, Audio, Video and Image Analysis Unit, the photograph submitted from the Illinois State identification photograph of OKUNOLA has "multiple similar class characteristics" as the aforementioned social media photos of OKUNOLA, however "due to the lack of visible unique

characteristics," the questioned images of Miracle Okunola and the known image of Miracle Okunola could not be identified or eliminated as being the same individual."

169. Facebook records indicated that the Facebook account with the display name "Miracle Okunola" was registered to "Miracle Okunola" with associated email address okunola.miracle@gmail.com and verified phone numbers XXX-XXX-1611, XXX-XXX-9336 and XXX-XXX-5025.

170. Google records indicated that the Google account with the display name "Okunola Miracle" was registered to "Okunola Miracle" with email address okunola.miracle1@gmail.com.

171. Further open source internet research on the name "Miracle Okunola" resolved to a Twitter account with the display name "Okunola Miracle."

172. Twitter records indicated that the aforementioned Twitter account was associated with the email account okunola.miracle1@gmail.com and phone number XXX-XXX-5025, linking these three social media accounts to the same individual.

173. According to court authorized pen register trap and trace data from on or about November 28, 2017, to on or about February 20, 2018, phone number XXX-XXX-1611 associated with OKUNOLA had communicated at least nine times with ETA by text message or voice call.

174. According to court authorized pen register trap and trace data on or about July 27, 2017, phone number XXX-XXX-9336, associated with OKUNOLA, had communicated at least six times with ETA by text message or voice call.

175. According to bank records, Nigerian Passport XXXXX8685 in the name of "Luke Johnson" was used to open five U.S. bank accounts, sometimes providing the phone number XXX-XXX-5025 and email address j.luke39@yahoo.com or zack.jacob90@yahoo.com in the opening documents. Additionally, the account opening documents included a scanned copy of a Nigerian Passport XXXXX8685 in the name of "Luke Johnson." This passport photograph also appears to be the same individual shown in known photographs of OKUNOLA.

176. Based on the fact that the photograph in the "Luke Johnson" passport is that of OKUNOLA, I believe the Nigerian passport XXXXX865, in the name "Luke Johnson" is fraudulent.

177. Email account records indicated that email address zack.jacob90@yahoo.com was registered to a "Zack Jacob" with associated phone number XXX-XXX-9336, which was previously associated to the Facebook account in the name of "Miracle Okunola."

178. Further research of a law enforcement database indicated that phone number XXX-XXX-9336 was linked to bank accounts in the names of "Zack Jacob" and "Abraham Tom" (or a variation thereof).

179. According to bank records, Nigerian Passport number XXXXX1312 in the name of "Jacob Zack" was used to open a bank account in the aforementioned fraudulent name, providing the email address j.luke39@yahoo.com in the opening documents, further corroborating the link between "Luke Johnson" and "Jacob Zack."

180. According to bank records and information obtained from a bank investigator, Nigerian Passport number XXXXX1877 in the name of "Abraham Tom" was used to open two bank accounts, utilizing phone numbers XXX-XXX-9336 and/or XXX-XXX-5025 as well as email addresses j.luke39@yahoo.com and/or tom_abraham@yahoo.com in the opening documents, further corroborating the link between "Luke Johnson" and "Abraham Tom."

181. Email account records indicated that email address j.luke39@yahoo.com was registered to "johnson luke" with a recovery phone number of XXX-XXX-9336.

182. Search warrant records for j.luke39@yahoo.com revealed several email notifications of bank account enrollments for "Luke Johnson" and/or "Jacob Zack" as well as emails with attachments containing .jpeg files of shipping labels addressed to third party individuals.

1. Employment Scam of Victim Q

183. A further review of ETA's Phones revealed a wire transfer of $2,984 from Victim Q's Bank of Oklahoma account to a JPMorgan Chase Bank checking account XXXXX3856 in the name "Luke Johnson."

184. According to bank records, the aforementioned JPMorgan Chase Bank account in the name "Luke Johnson" indicated a deposit of $2,984 on or about July 31, 2017.

185. In or around August and September 2018, Victim Q was interviewed by law enforcement. Victim Q stated, in summary, that in approximately June 2017, s/he was contacted online by and individual named "L. Johnson" on LinkedIn.

"L. Johnson" indicated that he was employed with a company called Fortune Finance and that he had funds to invest in Victim Q's enhanced oil recovery project. However, "L. Johnson" indicated that he needed help accessing his funds, which were "tied up" in Atlanta, Georgia. Victim Q stated that at some point s/he spoke with "L. Johnson" on the phone and agreed to help "L. Johnson" access his funds. Victim Q believed that "L. Johnson" was from somewhere in Europe, although "L. Johnson" claimed to have worked in California and Wyoming.

186. On or about September 6, 2018, Victim Q contacted law enforcement via email stating that s/he went to the Bank of Oklahoma to verify if s/he sent the aforementioned wire transfer of $2,984. The bank teller confirmed to Victim Q that s/he did indeed send the wire transfer, dated and signed by Victim Q on or about July 28, 2017. A copy of the wire transfer documentation was provided to law enforcement by Victim Q.

187. The wire transfer documentation provided by Victim Q appears identical to an image titled "wire-7-28-2017.pdf.pdf" from ETA's Phones, including a signature and date by Victim Q.

188. In or around December 2018, Victim Q sated to law enforcement, in summary, that the aforementioned $2,984 originated from a deposit into his/her Bank of Oklahoma bank account. This scheme is consistent with the activities of an unwitting money mule.

189. Additionally, ETA's Phones contained a BBM message regarding a wire transfer dated or about July 28, 2017, containing Victim Q's name address, sender

account number XXXXX3733, the recipient's account number XXXXX3856, routing number XXXXX0013, and the name "Luke Johnson."

190. Based on this evidence, the fact that ETA obtained this wire transfer information in an almost identical format to the actual wire transfer documentation and sent a BBM message with the co-conspirator's account information on or about the same date as the wire transfer was initiated by Victim Q, I believe that ETA was not only knowledgeable about this transaction, but was involved in this conspiracy to defraud through an online investment fraud scheme.

I. OLUROTIMI AKITUNDE IDOWU

191. A review of ETA's Phones revealed an image of a screenshot on or about December 28, 2016, of a TCF Bank "Account Agreement" in the fictitious name "Norman Isaac Williams" with an associated bank account number as well as additional communications in the form of text, BBM and/or Skype messages utilizing this identity to commit fraud.

192. Additionally, one of ETA's Phones contained an image of a voided check from a bank account in the name of "Norman I. Williams."

193. In the course of investigating the true identify of "Norman Williams," law enforcement obtained a forfeited United Kingdom Passport XXXXX9486 in the name of "Roy Frederick Benson." According to information obtained from bank personnel, this fraudulent passport was abandoned at a bank branch location by the passport holder on or about September 29, 2017, when he was questioned about potential fraud in the account of "Roy Benson." Furthermore, according to bank

personnel, accounts at this bank in the names of "Roy Benson," "Norman Williams," and OLUROTIMI IDOWU were being controlled by the same person. Bank personnel based this on a comparison of the passport photographs presented to open these accounts as well as video footage of ATM withdrawals conducted in sequence by the individual utilizing debit cards held in the accounts for "Roy Benson" and IDOWU.

194. In the course of investigating the true identify of "Roy Frederick Benson," law enforcement obtained an Illinois driver's license photograph of IDOWU. This photograph appeared to be the same individual as pictured in the United Kingdom Passport of Roy Frederick Benson.

195. On or about May 9, 2018, law enforcement officers employed by U.S. Customs and Border Protection conducted an examination of the United Kingdom Passport XXXXX9486 in the name of "Roy Frederick Benson" and determined that it was fraudulent.

196. According to information obtained from the British government, the above-referenced United Kingdom passport in the name of "Roy Frederick Benson" is fraudulent.

197. On or about June 18, 2018, CS-1 identified the photograph in the United Kingdom Passport XXXXX9486 in the name of "Roy Frederick Benson" as a person by the name of "Idol," stating that s/he met him in person through ETA, but does not know him well.

198. Law enforcement officers received bank records and still images of video footage pertaining to a bank account opened in the name of "Norman I. Williams" and

"Roy Benson." These documents included a scanned copy of a United Kingdom Passport XXXXX5431 in the name of "Norman Isaac Williams," a scanned copy of a United Kingdom Passport XXXXX9486 in the name of "Roy Frederick Benson," and at least three images of an individual inside a Fifth Third branch location, conducting teller transactions in the account of "Norman Williams." These three photos, dated on or about August 4, 2017, at 10:36:05 a.m. CST, on or about August 4, 2017, at 5:25:15 p.m. CST, and on or about August 5, 2017, at 10:53:02 a.m. CST, show what appears to be the same individual at a branch location teller conducting transactions in the account of "Norman Williams."

199. According to information obtained from the British government, the above-referenced United Kingdom passport in the name of "Norman Williams" is fraudulent.

200. In or around July 2018, CS-1 was shown a copy of the United Kingdom Passport photograph in the name of "Norman I. Williams," an Illinois driver's license photograph of IDOWU, and the three aforementioned branch teller still images. CS-1 identified the three branch teller still images conducting transactions in the account of "Norman Williams" by the name "Idol," the same person s/he previously identified from the United Kingdom Passport of "Roy Frederick Benson." CS-1 further stated that "Idol" is friends with ETA, and that CS-1 had seen "Idol" at least five times.[7]

[7] CS-1 could not identify the United Kingdom Passport photo in the name of "Norman I. Williams," stating that the quality of the image was too poor. Furthermore, CS-1 did not identify the Illinois driver's license photograph of IDOWU.

201. Based on my experience in this investigation, the passport photograph of "Roy Frederick Benson" and "Norman I. Williams," appear to be IDOWU.[8]

202. According to bank records and information obtained from bank investigators, United Kingdom Passport XXXXX5431 in the name of "Norman I. Williams" was used to open five U.S. bank accounts in the name "Norman Williams," sometimes providing the email address iswilliams@yahoo.com and/or phone number XXX-XXX-7998 in the account opening documents.

203. Additionally, according to bank records and information obtained from bank investigators, United Kingdom Passport XXXXX9486 in the name "Roy Benson" was used to open six U.S. bank accounts in the name "Roy Benson" sometimes providing the email address roybenson38@yahoo.com and/or phone number XXX-XXX-7998 in the account opening documents.

204. According to court authorized pen register trap and trace data authorized by the Chief Judge of the Northern District of Illinois, on or about August 31, 2018, phone number XXX-XXX-7998 communicated one time with ETA by voice call.

[8] According to the FBI's Forensic, Audio, Video and Image Analysis Unit, the photograph submitted from the Illinois driver's license photograph of IDOWU has "multiple similar class characteristics" as the United Kingdom Passport photograph of "Roy Benson," however "due to insufficient image detail and the lack of visible unique characteristics," the passport photograph of "Roy Benson" "could not be identified nor eliminated as being Olurotimi Idowu."

205. On or about July 31, 2018, email records indicated that email account iswilliams@yahoo.com is registered to "Isaac williams" with a recovery phone number of XXX-XXX-1381.

206. According to court authorized pen register trap and trace data from on or about April 24, 2017, to on or about November 28, 2017, phone number XXX-XXX-1381 communicated at least 52 times with ETA by text message or voice call.

207. Search warrant records for iswilliams@yahoo.com revealed several email notifications of bank account enrollments for "Norman Williams." Further email records reveal a message dated on or about January 2, 2017, sent from roybenson38@yahoo.com to iswilliams@yahoo.com stating "hello." I believe that IDOWU is using both accounts to perpetrate fraud under both the "Roy Frederick Benson" and Norman I. Williams" fake identities.

1. Business Email Compromise of Victim R

208. A review of ETA Phone 1 revealed an image of a screenshot from on or about December 28, 2016, of a TCF Bank "Account Agreement" in the fictitious name "Norman Isaac Williams" with associated bank account number as well as additional communications in the form of a text, BBM and/or Skype message utilizing this identity to commit fraud via a business email compromise.

209. Specifically, in or around July 2017, a series of Skype communications between ETA and a co-conspirator[9] contained what appeared to be email instructions to defraud Victim R through a business email compromise by having Individual J.S.,

[9] This is a different person than the unnamed co-conspirator discussed in section III.A.1.

who handled financial transactions for Victim R, wire $10,000 to a bank account in the name of "Norman I. Williams."

210. For example, on or about July 6, 2017, the co-conspirator sent ETA a Skype message stating "a beg no give anybody, na em i dey take work" [Please don't give this information to anybody, I'm using this for fraud]. ETA sent a return Skype message of "ok." ETA then sent another message to the co-conspirator asking where the money came from. The co-conspirator replied with "[Individual G.B.]. Make I paste you all the money the woman do today." Additionally, the co-conspirator sent ETA another message with instructions to send two wire transfers to two Bank of New York accounts, and then a third wire of $10,000 to an account in the name and account of "Norman I. Williams" at Fifth Third Bank, consistent with the scheme to commit fraud through a business email compromise.

211. Later that day, the co-conspirator sent ETA the following Skype messages, which were recovered from ETA Phone 1. These messages are almost identical to the emails Victim R received on or around that date from the comprised email account of his/her boss:

> Please wire $10,000 today from [Victim R] account ending in 3019. Please instruct the verification team to call me at XXX-XXX-7972. King Adekunle M'alwal The First, 7/6/2017. [Victim R], Please complete the following items first thing this morning from account ending in 3019. Please instruct your verification team to call me at [XXX-XXX]-7972. 1. Transfer $35,000 to [Individual L.B.]'s account ending in 9664. 2. Wire $5,000 to [Individual P.B.] Bank: Bank of New York ABA No.: XXXXX0018 Beneficiary: [LLC Entity] Account No: XXX-XXX238-5 ultimate Beneficiary: [Company R] Account No: XXXXX2188 Thank you, [Individual J.S.][.]

* * *

> Please wire $10,000 today from [Victim R] account ending in 3019. Please instruct the verification team to call me at XXX-XXX-7972. Norman I Williams Fifth third bank Acct#: XXXXXX8018 Routing #: XXXXXX909 Bank Address: [Chicago, Illinois] Thank you [Individual J.S.] ----- [Individual J.S.] XXX-XXX-7972 XXX-XXX-2564[.]

212. In or around July 2018, Individual J.S. was interviewed by law enforcement regarding the aforementioned business email compromise. Individual J.S. stated, in summary, that s/he worked directly for Victim R. Individual J.S. received multiple emails on or about July 5, 2017, and on or about July 6, 2017, from purportedly from Victim R requesting a $10,000 transfer be sent from Victim R's bank account to a bank account in the name of "Norman I Williams," at Fifth Third bank account XXXXXX8018 and routing number XXXXX3909. Individual J.S. further indicated that s/he initiated the wire transfer, but soon afterwards emailed Victim R's bank to have the transfer suspended once s/he realized that the emails from Victim R had been fraudulent.

213. According to emails provided by Individual J.S., Victim R's bank personnel replied to Individual J.S.'s email and confirmed a hold on the wire transfer of $10,000 and informed Individual J.S. that the routing number was invalid. Individual J.S. then canceled the wire request and Victim R's bank confirmed the transaction would not be processed.

214. Individual J.S. stated to law enforcement that Individual J.S. and Victim R communicated with each other about the above-referenced wire request. Individual J.S. confirmed that Victim R did not request the wire transfer, and did not send the above-referenced emails to Individual J.S. requesting the transfer. Based on

my training and experience, this is generally how business email compromise scams operate to attempt and/or defraud victims of money.

IV. MOVING PROCEEDS TO NIGERIA

215. A review of ETA's Phones revealed at least 300 communications in the form of a BBM messages between ETA and OGUNGBAIYE referencing monetary amounts, often times in the Nigerian currency Naira, with associated bank account numbers and/or bank account holder names located in Nigeria. Often times ETA further directed the transfer of money seemingly originating from the United States to OGUNGBAIYE's Nigerian bank account and then out to various individuals. In some instances, OGUNGBAIYE sent ETA a BBM image of the transfer from OGUNBAIYE's Nigerian bank account to an unknown co-conspirator's Nigerian bank account per ETA's instructions to show confirmation of the transfer to ETA. Based on the fact that ETA has no legitimate source of income, I believe OGUNGBAIYE's Nigerian bank account serves as a funnel account to move funds from the United States to end recipients in Nigeria at ETA's direction. During these communications between ETA and OGUNBAIYE, they discussed over 90,000,000 Naira, or approximately $147,000 in total.

216. In addition to funneling money overseas, according to records obtained from auto auction companies, ETA also owns a car company titled Samwas Partnership Limited. ETA has used this business to open up member accounts at U.S. auto auction dealers.

217. According to records obtained from auto auction companies, on at least three occasions, proceeds from bank accounts opened in fictitious names with fictitious passports were turned into money orders (totaling approximately $2,900) and were used to purchase at least two vehicles at auction under the Samwas Partnership Limited member ID, solely owned by ETA.

218. Additionally, ETA and several co-conspirators, to include LABIYI, ANIFOWOSHE, AKARIGIDI and EDJIEH, have conspired to move proceeds from bank accounts opened in fictitious names with fictitious passports into money orders which were then used to purchase vehicles on behalf of third party car companies located in Nigeria, consistent with the wire fraud scheme.

219. From approximately 2016 to 2018, according to a review of bank records obtained as part of this investigation identified numerous accounts that were opened in fictitious identities with fictitious passports. Based on these bank records, ETA and his co-conspirators appear to be responsible for defrauding victims from various online fraud scams of at least approximately $2 million.

V. CONCLUSION

220. Based on the foregoing, probable cause exists that the defendants conspired to commit a wire fraud scheme, in violation of Title 18, United State Code, Sections 1343 and 1349.

FURTHER AFFIANT SAYETH NOT.

ANDREW JOHN INNOCENTI
Special Agent, Federal Bureau of Investigation

SUBSCRIBED AND SWORN to before me on December 4, 2018.

JEFFREY COLE
United States Magistrate Judge