AFFIDAVIT OF SPECIAL AGENT AARON LINDAMAN IN SUPPORT OF AN APPLICATION FOR A CRIMINAL COMPLAINT AND SEARCH WARRANTS

I, Aaron Lindaman, state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent/Criminal Investigator with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"). I have been employed by HSI for approximately 13 years. Before that assignment, I was employed as a Border Patrol Agent for approximately 5 years. I am currently assigned to conduct investigations as the Special Agent in Charge of the Boston Office of HSI. As a Special Agent, I am authorized as an officer of the United States to conduct investigations and make arrests for offenses enumerated in Titles 8, 18, and 19 of the United States Code. I have received on-the-job training as well as HSI-sponsored training on these types of investigations. My investigations and training have included the use of surveillance techniques and the execution of search, seizure, and arrest warrants.

2. I am currently investigating MIKE OZIEGBE AMIEGBE, also known as Jacob Emmanuel, also known as James Emmanuel, also known as Kelvin Thomas, also known as Suen Wilson Edward, also known as James Dennis Awusi, also known as David Koffi, also known as Paul Douglas, also known as Brian Morgan, also known as John Isiah, for mail, wire and bank fraud, as well as conspiracy to commit those crimes, in violation of Title 18, United States Code, Sections 1341, 1343, 1344 and 1349, respectively; making a false statement to a bank, in violation of Title 18, United States Code, Section 1014; and money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957 (collectively, the "TARGET OFFENSES").

3. I submit this affidavit in support of a criminal complaint charging AMIEGBE with conspiracy to commit mail fraud, in violation of Title 18, United States Code, Section 1349. As further described below, I have probable cause to believe, and do believe, that beginning no later

than 2017 and continuing through at least 2020, AMIEGBE and others known and unknown conspired to use online "romance scams" to defraud victims by opening bank accounts under false identities, and inducing the victims to mail cashier's checks which AMIEGBE deposited into the fraudulent bank accounts.

4. I also submit this affidavit in support of applications for warrants to search the residence of AMIEGBE at 41 Supple Road, Apt. 1, Dorchester, Massachusetts (the "SUBJECT PREMISES"), as described in Attachment A-1, and a 2009 Toyota Camry, VIN 4T1BB46K29U090983, bearing MA 112VH1 (the "SUBJECT VEHICLE"), as described in Attachment A-2, because there is probable cause to believe that they contain evidence, fruits, and instrumentalities of the TARGET OFFENSES, as described in Attachment B.

5. The facts in this affidavit come from my personal observations and review of records, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested complaint and warrants, and does not set forth all my knowledge about this matter.

PROBABLE CAUSE TO BELIEVE THAT A FEDERAL CRIME WAS COMMITTED

6. Beginning no later than in or about 2017, and continuing through at least in or about 2020, AMIEGBE, together with those known and unknown, engaged in a scheme to defraud victims via online "romance scams"—a type of fraud that is enabled by the creation of fictitious profiles on online dating or social websites. Based on my training and experience, and my knowledge of this investigation, I am aware that individuals perpetrating romance scams use these online dating profiles to gain the trust of potential victims. Once that trust is gained, the perpetrators direct their victims to transfer money under false pretenses. Here, Victim 1 was induced to mail cashier's checks to aliases used by AMIEGBE, which AMIEGBE then deposited

into bank accounts opened using fake identification documents for those aliases. After the cashier's checks were deposited into the accounts, the money was generally withdrawn in cash within days.

Victim 1

7. Victim 1 is a 70-year-old woman residing in San Antonio, Texas.

8. Based on interviews with Victim 1 and other evidence I have reviewed as part of this investigation, I am aware that in or about November 2017, Victim 1 received a "friend request" via Facebook from an individual previously unknown to her, who went by the name "Gibson Banks." Victim 1 accepted the friend request, and shortly thereafter, "Banks" privately messaged her. Victim 1 and "Banks" subsequently began communicating on a regular basis. "Banks" told Victim 1 that he was a soldier in the U.S. Army conducting special operations missions across the world and was currently working in Syria. Victim 1 also communicated with "Banks" via text message and believed she was in a romantic relationship with "Banks," despite never meeting him in person or speaking to him on the telephone.

9. "Banks" told Victim 1 that he had come into millions of dollars while working in Iraq, and asked Victim 1 to send him money so that he could access his money overseas. "Banks" asked Victim 1 to travel to Belgium to retrieve a "consignment box" containing $24 million, and promised her part of the funds in return for her effort. In or about January 2018, Victim 1 traveled to Belgium, where she met an unknown man who went by the name "Daniel." Victim 1 brought $10,000 with her, which "Banks" had told her was needed to obtain the "consignment box." "Banks" told Victim 1 they needed more money to obtain the box, and she traveled to various Western Union locations around Antwerp and Brussels and used her credit cards to withdraw an additional approximately $26,000. Victim 1 gave the funds to "Daniel."

10. After Victim 1 returned to the United States, "Daniel" contacted her and said he needed another $92,000, which Victim 1 wired to "Daniel."

11. "Banks" continued to give Victim 1 excuses for needing more money, including that he purportedly needed funds to purchase special chemicals to remove ink from the currency, to give to authorities to get the funds out of the country, to cover costs of children who were sick, and to raise money to secure "Banks's" release from a Syrian prison.

12. For example, in or about the fall and winter of 2019, Victim 1 sent $70,000 in cashier's checks to "James," a friend of "Banks," who was purportedly raising money to secure "Banks's" release from prison. During that period, Victim 1 communicated with "James" approximately twice per week.

13. In total, Victim 1 sent more than $720,000 in funds at the direction of "Banks" or his associates.

x7685 TD Bank Account

14. On or about October 18, 2019, an account ending in x7685 was opened at a TD Bank branch in Reading, Massachusetts, in the name of Jacob Emmanuel. In order to open the account, the person purporting to be Jacob Emmanuel presented a South African passport, bearing the number A04719653, and showing a date of birth of February 16, 1979.

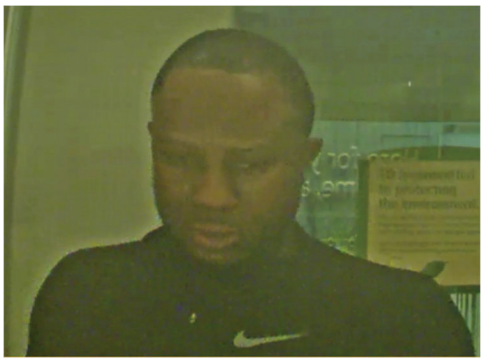
15. I have queried Customs and Border Protection ("CBP") border crossing databases for information about Jacob Emmanuel, with a date of birth of February 16, 1979 and South African passport #A04719653. No information was found, which leads me to believe that the identification is fake and/or that Jacob Emmanuel did not enter the United States at a designated Port of Entry.

16. Although TD Bank surveillance images from the opening of the x7685 account depict a man who does not appear to be AMIEGBE opening the account, surveillance images from on or about October 19, 2019—the day after the x7685 account was opened—show a man who appears to be AMIEGBE depositing a $10,000 cashier's check from Victim 1 and made out to Jacob Emmanuel into the x7685 account:

Notably, AMIEGBE appears to be wearing the same sweatshirt in a photo he submitted with his I485 application for permanent residence in the United States:

17. The $10,000 cashier's check deposited into the x7685 account was promptly withdrawn in the form of a $7,600 cash withdrawal on or about October 24, 2019 and a $2,350 cash withdrawal on or about October 25, 2019. No surveillance exists for the October 24, 2019 withdrawal; however TD Bank surveillance of the October 25, 2019 withdrawal appears to depict the same man who opened the x7685 account, who is not AMIEGBE.

18. On or about October 29, 2019, TD Bank surveillance images show a man who appears to be AMIEGBE depositing a $14,000 cashier's check from Victim 1 and made out to Jacob Emmanuel into the x7685 account in the name of Jacob Emmanuel:



19. The $14,000 cashier's check deposited into the x7685 account was promptly withdrawn in the form of a $7,780 cash withdrawal on or about November 2, 2019 and a $6,180 cash withdrawal on or about November 4, 2019. No surveillance exists for the November 2, 2019 withdrawal; however TD Bank surveillance of the November 4, 2019 withdrawal appears to depict the same man who opened the x7685 account, who is not AMIEGBE.

20. Another individual, who investigators have identified as Kofi Osei, appears on TD Bank surveillance using the x7685 account on four occasions in or about January 2020. In February 2021, Osei was indicted in the United States District Court for the District of Massachusetts on charges of making a false statement to a bank, in violation of Title 18, United States Code, Section 1014, wire fraud, in violation of Title 18, United States Code, Section 1343, and money laundering, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i), in connection with his role in an online romance scam. *See United States v. Osei*, No. 21-cr-10064-IT-DLC.

21. Other individuals, who are unknown to investigators, also appear in TD Bank surveillance using the x7685 account through at least May 2020.

22. Between on or about May 7, 2020 and on or about May 22, 2020, multiple deposits from the Massachusetts Department of Unemployment Assurance for pandemic unemployment assistance totaling approximately $25,355 in the names of multiple individuals were deposited into the x7685 account.

x6539 TD Bank Account

23. On or about December 6, 2019, an account ending in x6539 in the name of James Emmanuel was opened at a TD Bank branch in Reading, Massachusetts. In opening the account, the person purporting to be James Emmanuel used a South African passport bearing the number A05837624, and showing a date of birth of February 17, 1984.

24. Both the Jacob Emmanuel x7685 and the James Emmanuel x6539 accounts listed 125 Norfolk Street, Boston, Massachusetts as the customer's address.

25. I queried CBP border crossing databases for information about James Emmanuel, with a date of birth of February 17, 1984 and South African passport #A05837624. No information was found, which leads me to believe that the identification is fake and/or that James Emmanuel did not enter the United States at a designated Port of Entry.

26. TD Bank did not have surveillance images from the opening of the x6539 account in the name of James Emmanuel. However, on or about December 7, 2019—the day after the x6539 account was opened—TD Bank surveillance images show a man who appears to be AMIEGBE depositing a $5,000 cashier's check from Victim 1 into the x6539 account in the name of James Emmanuel:

27. The $5,000 cashier's check deposited into the x6539 account was withdrawn in the form of several ATM cash withdrawals totaling $2,500 in or about December 2019, and a $2,500 teller withdrawal on or about December 18, 2019. No surveillance exists for these withdrawals.

28. On or about January 3, 2020, a cashier's check for $13,800 drawn on Victim 1's account was deposited into the x6539 James Emmanuel account. There are no surveillance photos of this transaction.

29. However, on or about January 6, 2020, investigators conducted an examination of the garbage placed on or near the curb of the SUBJECT PREMISES.[1] In so doing, investigators found an empty United Parcel Service ("UPS") envelope dated January 2, 2020 from Victim 1 addressed to James Emmanuel of 63 Draper Street, Dorchester, Massachusetts. Based on my training and experience and my knowledge of this investigation, I believe this was the envelope in

[1] Investigators coordinated with Castle Waste Management, the company responsible for garbage service at the SUBJECT PREMISES. The garbage truck that was used for this operation was empty, and was only used to pick up the garbage collected from the SUBJECT PREMISES. Following the garbage pickup by Castle Waste Management, investigators took custody of the garbage. I am aware that there are two apartments within the SUBJECT PREMISES. Investigators attempted to separate bags of trash that appeared to come from Apartment 2 from those that appeared to come from Apartment 1 by, for example, checking the address on envelopes and circulars in the bags. Once sorted, investigators did not examine the bags that appeared to have come from Apartment 2 and discarded them.

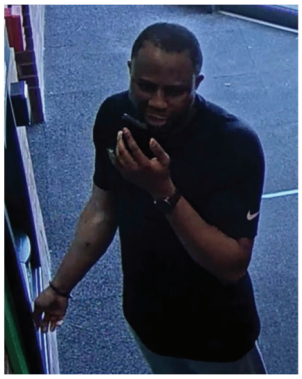
which Victim 1 sent the $13,800 cashier's check to the person Victim 1 believed was James Emmanuel. Additionally, as detailed below in Paragraph 36, I am aware that bank accounts opened at TD Bank and Citizens Bank using the Jacob Emmanuel and James Emmanuel identities list 63 Draper Street, Boston, Massachusetts as the customer's address.

30. The bulk of the cashier's check deposited into the x6539 account was promptly withdrawn in the form of a $6,000 teller withdrawal on or about January 6, 2020, and a $3,000 teller withdrawal on or about January 9, 2020. There were also smaller ATM cash withdrawals. No surveillance exists for these withdrawals.

31. On or about May 12, 2020, TD Bank surveillance images show a man who appears to be AMIEGBE depositing a $3,500 cashier's check from Victim 1 into the x6539 account in the name of James Emmanuel:

TD Bank surveillance images of the vehicle depicted above confirm—based on the make, model, color, and license plate—that the vehicle is the SUBJECT VEHICLE.

32. The $3,500 cashier's check deposited into the x6539 account was promptly withdrawn in the form of eight separate $400 ATM withdrawals between on or about May 14, 2020 and on or about May 18, 2020. TD Bank surveillance of one of the withdrawals, on or about May 17, 2020, appears to depict AMIEGBE:



AMIEGBE

33. As noted, I believe that the man in the surveillance photos above transacting in the x7685 Jacob Emmanuel and x6539 James Emmanuel accounts is AMIEGBE based on my personal surveillance of him and his use of the SUBJECT VEHICLE, which is registered to AMIEGBE, to conduct transactions in those accounts.

34. Additionally, TD Bank captured IP addresses used to access the x7685 and x6539 accounts. For example, on or about May 29, 2020 at approximately 7:08 p.m., the IP address 98.217.184.42 was used to access the x7685 account in the name of Jacob Emmanuel, and on or about June 1, 2020, at approximately 1:54 p.m., the same IP address was used to access the x6539 account in the name of James Emmanuel. Comcast records confirm that, on or about both of those dates and times, the IP address was registered to the SUBJECT PREMISES, although the subscriber is not AMIEGBE.

35. On or about August 28, 2020, investigators confirmed that the IP address 98.217.184.42 is secure, meaning that the individual(s) accessing the x7685 and x6539 accounts from that IP address were either directly connected to the Internet from inside the SUBJECT PREMISES, or were privy to the password and login information for any wireless networks used to access the Internet at the SUBJECT PREMISES. Specifically, investigators searched for wireless networks in the area of the SUBJECT PREMISES. Standing approximately 15 feet from

the SUBJECT PREMISES, at the intersection of Supple Road and Normandy Street, all wireless networks with a "good" to "excellent" signal strength were revealed to be WPA2-PSK secured—that is, password protected and not open to public use. There were two unsecured (that is, not password protected) networks with a "fair" signal strength, but neither had the IP address 98.217.184.42.

36. In addition to the x7685 account in the name of Jacob Emmanuel and the x6539 account in the name of James Emmanuel, the investigation to date has linked AMIEGBE with the following assumed names and accounts, all opened with passports that appear to be fake:

Alias	Bank	Last Four Digits of Account	Address Associated with Account	Telephone Number Associated with Account	Email Address Associated with Account
Jacob Emmanuel	TD Bank	0792	125 Norfolk St. Boston, MA 02124		Autoshop147@mail.com
Jacob Emmanuel	TD Bank	6683 0824	63 Draper St. Boston, MA 02122	857-204-5585	jjemanuel0147@gmail.com
Jacob Emmanuel	Bank of America	3113	125 Norfolk St., Apt. 1 Boston, MA 02124	646-541-9416	afriqueautosale@mail.com
James Emmanuel	TD Bank	6445	125 Norfolk St. Boston, MA 02124		Emmacarshop147@gmail.com
James Emmanuel	Citizens Bank	3948 4514	63 Draper St., Apt. 1 Boston, MA 02122		
Paul Douglas	TD Bank	5706 2785	70 Readville St., Apt. C Hyde Park, MA 02136		Workbox0147@gmail.com
Paul Douglas	Citizens	2106	18 Hendry St. Boston, MA 02122		

Kelvin Thomas	TD Bank	6073 0075	12 East St. Dorchester, MA 02124		Workbox014701@gmail.com
Kelvin Thomas	Citizens	7346 1669	125 Norfolk St. Boston, MA 02124		
Kelvin Thomas	Santander	7646 0711	125 Norfolk St. Boston, MA 02124	404-547-2515	Workbox014701@gmail.com
John Isiah	TD Bank	1307 3211	12 East St., Apt. 1 Dorchester, MA 02124		kglake@yahoo.com
Isiah John	Citizens	0268	18 Hendry St., Apt. 2 Boston, MA 02122		
Brian Morgan	TD Bank	9589 8674	125 Norfolk St. Boston, MA 02124		Workbox014701@gmail.com
James Dennis Awusi	Santander	7162	75 Madina Accra, Ghana	401-688-2439	Scotlinda61@gmail.com
James Dennis Awusi	TD Bank	6761 7151	172 Washington St., Apt. 4 Boston, Lynn, MA 01902	646-875-1258	Autoshop121@gmail.com
James Dennis Awusi	Bank of America	3225	172 Washington St., Apt. 4 Lynn, MA 01902		
Suen Edward	Eastern Bank	9519 7548	172 Washington St., Apt. 14 Lynn, MA 01902		
Suen Wilson Edward	Santander	9328 2842	172 Washington St., Apt. 14 Lynn, MA 01902	646-875-1258	kglake@yahoo.com
Suen Wilson Edward	TD Bank	4013 5447 9349	209 Lowell St. Peabody, MA 01960		kglake@yahoo.com

David Koffi	Bank of America	1200	2001 Commonwealth Ave., Apt. 2 Brighton, MA 02135		
David Koffi	Santander	7553	78 Medina Accra, Ghana	646-875-1258	Lakeshop121@gmail.com

THE PREMISES CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES

37. I also have probable cause to believe that the premises to be searched contain fruits, evidence, and instrumentalities of violations of the TARGET OFFENSES, as described in Attachment B.

The SUBJECT PREMISES

38. The SUBJECT PREMISES is a two-family, two-story home. There is a vestibule at the front door that leads to two apartments. The interior apartment doors are not marked. However, postal records for the SUBJECT PREMISES reflect that the door on the right is the entry for Apartment 1.

39. Additionally, there is a back door that provides entry and exit to Apartment 1. Investigators have observed AMIEGBE exiting the building through this back door on several occasions.

40. According to postal records, AMIEGBE receives mail at the SUBJECT PREMISES.[2]

41. Additionally, investigators have conducted surveillance of the SUBJECT PREMISES and have observed the SUBJECT VEHICLE parked at the SUBJECT PREMISES,

[2] According to postal records, another individual, Stephen Amiegbe, receives mail at the SUBJECT PREMISES. However, records reflect that Stephen Amiegbe enlisted in the U.S. Army and is currently stationed outside of Massachusetts.

and AMIEGBE entering and exiting the SUBJECT PREMISES. For example, on March 22, 2021, investigators observed AMIEGBE leave through the front door of the SUBJECT PREMISES and get into a black 2012 Toyota Highlander, Massachusetts license plate 9HA861, which is also registered to AMIEGBE. While AMIEGBE uses both the SUBJECT VEHICLE and the Toyota Highlander, investigators have more often observed him in the SUBJECT VEHICLE.

42. In my training and experience, I know that locations occupied by perpetrators of fraud schemes frequently contain evidence that will aid in establishing the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the government to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. Based on the information set forth herein, including the fact that AMIEGBE resides at the SUBJECT PREMISES, I believe it is likely that the SUBJECT PREMISES will contain evidence of the TARGET OFFENSES, including without limitation clothing matching that worn in surveillance images; passports and other identification documents in the names of Jacob Emmanuel, James Emmanuel, and others used to open bank accounts; AMIEGBE'S true passport and identification documents; passport stamps or other materials used to create counterfeit passports and other identification documents; bank account opening documents, monthly statements, debit cards, ATM receipts, and other banking materials in the names of Jacob Emmanuel, James Emmanuel, and others; bank account opening documents, monthly statements, debit cards, ATM receipts, and other banking materials in AMIEGBE'S name; receipts for purchases made using the Jacob Emmanuel, James Emmanuel, and other fraudulently opened accounts; computers and telephones used to communicate with victims; computers and telephones used to communicate with co-conspirators; and cash and money orders.

43. Although a number of months have passed since the bank accounts identified above have been active, I believe evidence of the TARGET OFFENSES will nevertheless be found at the SUBJECT PREMISES. For example, in my experience, people tend to keep clothing, like the clothing worn in surveillance photos, for many years and not discard it. While AMIEGBE may have replaced his computer or phone since May 2020, in my training and experience, individuals tend to "back up" their computers and phones to external drives, which may be found in the SUBJECT PREMISES, or in the "cloud" and downloaded to a new computer or phone.

The SUBJECT VEHICLE

44. Bank surveillance images depict AMIEGBE transacting at drive-up ATMs in the SUBJECT VEHICLE, a 2009 Toyota Camry bearing Massachusetts license plate 112VH1. This vehicle is registered to AMIEGBE. Investigators have observed AMIEGBE using the SUBJECT VEHICLE on many occasions and it is regularly parked outside the SUBJECT PREMISES.

45. Additionally, on or about May 30, 2019, investigators observed AMIEGBE driving another apparent co-conspirator ("CC-1") in the SUBJECT VEHICLE. AMIEGBE drove CC-1 to various banks, including a Santander Bank branch in Chelsea, Massachusetts. CC-1 entered the bank and opened up an account ending in x8257 in the name of Maxwell Howard, using a United Kingdom passport bearing the number 375329546 and date of birth of January 10, 1976. I queried ("CBP") border crossing databases for information about Maxwell Howard with a date of birth of January 10, 1976 and United Kingdom passport #375329546. No information was found, which leads me to believe that the identification is fake and/or Maxwell Howard did not enter the United States at a designated Port of Entry. Notably, the address provided for the account was 63 Draper

Street, Boston, Massachusetts, which is the same address on the January 2, 2020 envelope from Victim 1 found in the trash at the SUBJECT PREMISES.[3]

46. As with the residences in which they live, it is my experience that the vehicles driven by perpetrators of fraud schemes frequently contain evidence of the criminal conduct under investigation. Accordingly, I believe it is likely that the SUBJECT VEHICLE will contain evidence of the TARGET OFFENSES, including many of the same items I would also expect to find in the SUBJECT PREMISES, such as cash; passports and other identification documents in the names of Jacob Emmanuel, James Emmanuel, and others used to open bank accounts; AMIEGBE'S true passport and identification documents; passport stamps or other materials used to create counterfeit passports and other identification documents; bank account opening documents, monthly statements, debit cards, ATM receipts, and other banking materials in the names of Jacob Emmanuel, James Emmanuel, and others; bank account opening documents, monthly statements, debit cards, ATM receipts, and other banking materials in AMIEGBE'S name; receipts for purchases made using the Jacob Emmanuel, James Emmanuel, and other fraudulently opened accounts; and clothing matching clothing worn in surveillance images.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

47. From my training, experience, and information provided to me by other agents, I am aware that individuals frequently use computers to create and store records of their actions by communicating about them through email, instant messages, and updates to online social networking websites; drafting letters; keeping their calendars; arranging for travel; storing

[3] Additional accounts ending in x7494 and x3969 in the name of Maxwell Howard were opened at Citizens Bank. During the surveillance of AMIEGBE, he also drove CC-1 to a Citizens Bank branch to open an account ending in x1989 in the name of Mark Nelson.

pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

48. Based on my training, experience, and information provided by other law enforcement officers, I know that many cell phones (which are included in Attachment B's definition of "hardware") can now function essentially as small computers. Phones have capabilities that include serving as a wireless telephone to make audio calls, digital camera, portable media player, GPS navigation device, sending and receiving text messages and emails, and storing a range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence of communications and evidence that reveals or suggests who possessed or used the device.

49. Here, perpetrators communicated with Victim 1 via Facebook. They also communicated with Victim 1 over email and text message.

50. Based on my training, experience, and information provided by other law enforcement officers, I know that "romance scams" often involve multiple conspirators. Some conspirators communicate with victims, and other conspirators set up accounts to receive and withdraw victim funds. Often, these conspirators communicate with each other over email or messaging applications to notify (a) the conspirators communicating with victims of the bank account information of where to send funds, and (b) the conspirators withdrawing funds from the accounts when to expect funds, so that they can be withdrawn quickly.

51. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years

after they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.

b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.

d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache." The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are

overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

e. Data on a storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about when the dates files were created and the sequence in which they were created, although this information can later be falsified.

52. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the government to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (*e.g.*, registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crimes under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (*e.g.*, a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (*e.g.*, Internet searches indicating criminal planning), or consciousness of guilt (*e.g.*, running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

53. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

54. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

55. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

56. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media ("computer equipment") be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

a. The volume of evidence that storage media such as hard disks, flash drives, CDs, and DVDs can store is the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis onsite.

b. Technical requirements analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even "hidden," deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a "booby trap."

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

57. The premises may contain computer equipment whose use in the crimes or storage of the things described in this warrant is impractical to determine at the scene. Computer

equipment and data can be disguised, mislabeled, or used without the owner's knowledge. In addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

58. The law enforcement agents will endeavor to search and seize only the computer equipment which, upon reasonable inspection and/or investigation conducted during the execution of the search, reasonably appear to contain the evidence in Attachment B because they are associated with (that is used by or belong to) AMIEGBE. If, however, the law enforcement agents cannot make a determination as to use or ownership regarding any particular device, the law enforcement agents will seize and search that device pursuant to the probable cause established herein.

59. This warrant authorizes a review of electronically stored information, communications, other records, and information seized, copied or disclosed pursuant to this warrant to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, HSI may deliver a complete copy of the seized, copied, or disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

UNLOCKING A DEVICE USING BIOMETRIC FEATURES

60. I know from my training and experience, as well as from information found in publicly available materials, that some models of cellphones made by Apple and other manufacturers offer their users the ability to unlock a device via the use of a fingerprint or through facial recognition, in lieu of a numeric or alphanumeric passcode or password.

61. On the Apple devices that have this feature, the fingerprint unlocking feature is called Touch ID. If a user enables Touch ID on a given Apple device, he or she can register up to five fingerprints that can be used to unlock that device. The user can then use any of the registered fingerprints to unlock the device by pressing the relevant finger(s) to the device's Touch ID sensor. In some circumstances, a fingerprint cannot be used to unlock a device that has Touch ID enabled, and a passcode must be used instead, such as: (1) when more than 48 hours has passed since the last time the device was unlocked and (2) when the device has not been unlocked via Touch ID in 8 hours and the passcode or password has not been entered in the last 6 days. Thus, in the event law enforcement encounters a locked Apple device, the opportunity to unlock the device via Touch ID exists only for a short time. Touch ID also will not work to unlock the device if (1) the device has been turned off or restarted; (2) the device has received a remote lock command; or (3) five unsuccessful attempts to unlock the device via Touch ID are made.

62. The passcode that would unlock device(s) found during the search of the Subject Premises is not currently known to law enforcement. Thus, it may be useful to press the finger(s) of the user(s) of the device(s) to the device's fingerprint sensor or to hold the device up to the face of the owner in an attempt to unlock the device for the purpose of executing the search authorized

by this warrant. The government may not otherwise be able to access the data contained on those devices for the purpose of executing the search authorized by this warrant.

63. In my training and experience, the person who is in possession of a device or has the device among his or her belongings at the time the device is found is likely a user of the device. However, in my training and experience, that person may not be the only user of the device whose fingerprints are among those that will unlock the device and it is also possible that the person in whose possession the device is found is not actually a user of that device at all. Furthermore, in my training and experience, I know that in some cases it may not be possible to know with certainty who is the user of a given device, such as if the device is found in a common area of a premises without any identifying information on the exterior of the device. Thus, it may be necessary for law enforcement to have the ability to require any occupant of the Subject Premises to press their finger(s) against the sensor of the locked device(s) or place the devices in front of their faces in order to attempt to identify the device's user(s) and unlock the device(s).

64. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of individuals found at the Subject Premises to the sensor of the devices or place the devices in front of their faces for the purpose of attempting to unlock the device to search the contents as authorized by this warrant.

CONCLUSION

Based on the information described above, I have probable cause to believe that AMIEGBE has conspired to commit mail fraud, in violation of Title 18, United States Code, Section 1349, and that evidence, fruits, and instrumentalities of that crime, and the other TARGET OFFENSES described in Attachment B, are contained within the premises described in Attachments A-1 and A-2. Sworn to under the pains and penalties of perjury,

Aaron Lindaman
Special Agent
Homeland Security Investigations

Subscribed and sworn to before me on March 24, 2021 by telephone,

Hon. Donald L. Cabell
United States Magistrate Judge