AFFIDAVIT

I, MICHAEL LIVINGOOD, state:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been so employed since June 2016. I am assigned to the Economic Crimes Squad in the FBI's Boston, Massachusetts Field Office. My duties include investigating money laundering, wire fraud, and internet fraud schemes. I have participated in the execution of warrants involving the search and seizure of computers, computer equipment, and electronically stored information. Before becoming a Special Agent, I was an Intelligence Analyst for the FBI and supported investigative work on a variety of federal crimes, including crimes against children, transnational organized crime, and money laundering. I have received specialized training in investigating financial frauds and money laundering. I hold a master's degree in human services. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

2. This affidavit is being submitted in support of an application for:

   (a) a criminal complaint charging AUGUSTINE OSEMWEGIE ("OSEMWEGIE") with conspiracy to commit bank and wire fraud, in violation of 18 U.S.C. § 1349:

   (b) a warrant to search OSEMWEGIE's residence at 104 Thacher Street, Milton, Massachusetts (the "SUBJECT PREMISES"), as described in Attachment A to the proposed warrant;

because there is probable cause to believe both that OSWEMWEGIE violated 18 U.S.C. § 1349 and that the SUBJECT PREMISES contain evidence, fruits and instrumentalities of violations of federal law, including 18 U.S.C. §§ 371 (conspiracy), 1343 (wire fraud), 1344 (bank fraud), 1349 (attempt and conspiracy), 1956 and 1957 (money laundering and conspiracy to commit money

laundering) and 1960 (operating an unlicensed money transmitting business) (collectively, the "TARGET OFFENSES"), as described in Attachment B to the proposed warrant.

3. 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 sufficient probable cause for the requested complaint and search warrant and does not set forth all my knowledge about this matter.

PROBABLE CAUSE THAT OSEMWEGIE COMMITTED FEDERAL CRIMES

4. As set forth below, there is probable cause to believe that, between approximately October 2018 and the present, OSEMWEGIE, together with others known and unknown, conspired to commit bank and wire fraud, in violation of 18 U.S.C. § 1349, through a series of fraud scams. OSEMWEGIE participated in these schemes by laundering proceeds from them into off-shore accounts using a business front that he controlled.

5. As described in greater detail below, the investigation has revealed that OSEMWEGIE acquired the proceeds of various frauds from co-conspirators, which he caused to be transferred overseas in various ways, including, for example, by using the proceeds to purchase used vehicles, which he then shipped to Nigeria and sold. The proceeds from the sales in Nigeria were then paid out to other co-conspirators, allowing those involved in the conspiracy to circumvent detection and regulation of their funds transfer by the banking system. OSEMWEGIE charged a fee of approximately 10 percent of the fraud proceeds that he transferred.

6. According to the Secretary of the Commonwealth of Massachusetts, OSEMWEGIE is the president of Ejad Auto Sales, which was registered on May 2, 2019. The company website identifies the following individuals:

Position	Name
PRESIDENT	AUGUSTINE OSEMWEGIE SR
TREASURER	JOEL OSEMWEGIE
SECRETARY	EDOSA OSEMWEGIE JR
CEO	TREASURE OSEMWEGIE
ASSISTANT SECRETARY	DESTINY OSEMWEGIE
DIRECTOR	AUGUSTINE OSEMWEGIE SR

According to records and databases available to the FBI, the other individuals listed on the registration of Ejad Auto Sales are OSEMWEGIE's children and family members.

7. TD Bank N.A., one of the affected banks, is a financial institution within the meaning of 18 U.S.C. § 20.

OSEMWEGIE and CW-1

8. In or about the summer of 2020, CW-1 pleaded guilty to one count of mail and wire fraud conspiracy, in violation of 18 U.S.C. § 1349, and one count of unlawful monetary transactions, in violation of 18 U.S.C. § 1957. In connection with its plea, CW-1 agreed to cooperate with the government's investigation.

9. CW-1 spoke with investigators and described a fraud and money laundering enterprise in which CW-1 and others participated that included, but was not limited to, the following:

a. Various individuals, including CW-1, opened and provided bank accounts to receive the proceeds from various frauds. Sometimes they used accounts in their own names, and sometimes they used accounts opened with false identifications, including fake passports.

b. CW-1 and other conspirators used the services of OSEMWEGIE to transfer some of the proceeds of the frauds from Massachusetts to Nigeria.

c. There was a network of co-conspirators in Nigeria, to whom CW-1 provided U.S.-based bank accounts that could be used to receive fraud proceeds. CW-1 generally charged a 15 percent fee of the total amount that came into an account that he controlled.

d. CW-1 withdrew fraud funds from the accounts he controlled in cash. After withdrawing the cash, CW-1 took the remaining proceeds (*i.e.*, less his fee) to OSEMWEGIE. OSEMWEGIE took a percentage of the funds as his fee, which was usually 10 percent or more. OSEMWEGIE then paid out the remaining funds to CW-1's Nigerian-based bank accounts. It took OSEMWEGIE only one to two days to pay the funds out to the requested Nigerian-based bank account. CW-1 then paid its Nigeria-based co-conspirators with the funds OSEMWEGIE sent.

e. OSEMWEGIE was able to pay out to Nigeria-based bank accounts so quickly because OSWEMWEGIE moved money to Nigeria by shipping cars. OSEMWEGIE used the cash proceeds that CW-1 and others gave him to buy vehicles at various used car auto auctions in Massachusetts and elsewhere, and then shipped the vehicles to Nigeria. CW-1 witnessed this activity. OSEMWEGIE sold the vehicles to dealers in Nigeria, who pay him naira (Nigerian national currency) into his Nigeria-based bank accounts. OSEMWEGIE then provided the proceeds of the Nigerian car sales as CW-1 directed.

f. CW-1 communicated with OSEMWEGIE by messages and calls to telephone number 617-997-7687.

OSEMWEGIE's Business Activity Corroborates CW-1's Reporting

10. According to export data from U.S. Customs and Border Patrol ("CBP"), between on or about November 8, 2018 and August 13, 2021, Ejad Auto Sales[1] exported 183[2] vehicles from the United States to Nigeria, and 2 vehicles to Cotonou, Benin.[3] The total value declared to CBP for these vehicles was approximately $1,117,320, which is an approximate average of $6,105 per vehicle. Between October 5, 2018 and June 8, 2020, OSEMWEGIE, in his own name, exported 33 vehicles from the United States to Nigeria. The total value declared to CBP for these vehicles was approximately $163,055, which is an approximate average of $4,941 per vehicle.

11. The activity in OSEMWEGIE's and Ejad Auto Sales' bank accounts is also consistent with CW-1's reporting. Records for these accounts show the purchase of vehicles in the United States using cash and money orders deposited into the accounts from within the United States, and no payments to the accounts that appear to be from Nigeria. For example, in a one-year period between August 2019 and August 2020, records for OSEMWGIE's and Ejad Audo Sales' accounts show the following:

Chase Bank – Ejad Auto Sales

a. Over $120,000 in purchases at auto auctions and for export costs
b. Over $57,000 deposited in cash
c. Over $35,000 deposited in money orders

---

[1] In some instances, the individual name listed on the export shipment for Ejad Auto Sales is OSEMWEGIE, and in others, individuals known and unknown to the investigator; however, other information reported to CBP, such as the reported address, suggests all referenced shipments are on behalf of OSEMWEGIE's business.

[2] Ejad shipped 11 vehicles in 2018 and 2019, with the remaining 172 shipments occurring in 2020 and 2021.

[3] The port of Cotonou is located in West Africa and is approximately 77 miles from the port in Lagos, Nigeria.

TD Bank – Ejad Auto Sales

d. Over $27,000 in purchases at auto auctions and export costs
e. Over $12,000 deposited in cash
f. Over $8,000 deposited in money orders

TD Bank – OSEMWEGIE personal account

g. Over $58,000 in purchases at auto auctions and export costs
h. Over $86,000 deposited in cash
i. Over $14,000 deposited in money orders

Total purchases at auto auctions and export costs: over $205,000

Total cash and money order deposits: over $212,000

12. During this same one year period (August 2019 to August 2020), there was no evidence of incoming funds from Nigeria that could represent proceeds from the sale of the vehicles shipped to Nigeria.

13. According to CBP records, during this time period, OSEMWEGIE and Ejad Auto Sales exported 42 vehicles with declared values totaling over $176,000.

Money Transmitting Businesses and Informal Value Transfer Systems

14. Based on my training and experience investigating financial crimes, I am aware that shipping vehicles as a method of money transmitting to a foreign country is commonly referred to as an Informal Value Transfer System ("IVTS"). According to the Financial Crimes Enforcement Network ("FinCEN"), IVTS may legally operate in the United States, so long as they abide by applicable state and federal laws. This includes registering with FinCEN and complying with the anti-money laundering and financing provisions of the Bank Secrecy Act, which would include reporting known or suspected money laundering activity to FinCEN. On

August 18, 2021, I searched FinCEN's online database of registered money transmitters and did not locate a registration for either OSEMWEGIE or Ejad Auto Sales.

15. Massachusetts law (M.G.L. chapter 169) defines foreign remittance activity as "receiving deposits of money for the purpose of transmitting the same or equivalents thereof to foreign countries," so the license requirement is not dependent on how the value gets from one location to another, but instead is triggered by the act of accepting funds in Massachusetts and making the equivalent available for the beneficiary abroad. Therefore, IVTS activity would be allowed under the Massachusetts statute, but would require being registered here as a Licensed Money Transmitter. On August 18, 2021, I learned from the Massachusetts Division of Banks that OSEMWEGIE is not a Licensed Money Transmitter.

16. Based upon my review of numerous bank records and open source research, international wire fees for a money transfer generally average between $35 and $65 per wire.

CW-1 Introduced OSEMWEGIE to a CHS

17. On September 4, 2020, CW-1 placed a call to OSEMWEGIE. Agents were present for and recorded this call. In sum and substance, CW-1 told OSEMWEGIE that he was going to introduce OSEMWEGIE to a friend named "Shola" (the Confidential Human Source or "the CHS").

18. On September 4, 2020, the CHS used a phone provided to him by the FBI to communicate with OSEMWEGIE using WhatsApp to telephone number 617-997-7687—the phone number that CW-1 attributed to OSEMWEGIE.

19. Between September 4, 2020 and on or about September 17, 2020, the CHS recorded several conversations with OSEMWEGIE about transferring funds received from fraud schemes out of the United States, including as described below.[4]

20. On or about September 6, 2020, the CHS spoke with OSEMWEGIE on a recorded call and told OSEMWEGIE that he was expecting money to come in and he wanted OSEMWEGIE's assistance in sending money to Bitcoin or to an account off-shore. During the conversation, OSEMWEGIE expressed hesitancy to discuss business over the phone, but he continued after the CHS reassured OSEMWEGIE that WhatsApp was a safe platform for their conversation. OSEMWEGIE assured the CHS he would get his money quickly. The CHS and OSEMWEGIE agreed to meet once the CHS's money arrived. Near the end of the conversation, the CHS told OSEMWEGIE that the CHS' money was "not legit,".

21. On or about September 16, 2020, while organizing a place to meet on a recorded call, the CHS and OSEMWEGIE how much OSEMWEGIE would charge the CHS to send the money overseas. OSEMWEGIE proposed charging 40 percent, and the CHS countered by offering 10 percent.

Meeting Between the CHS and OSEMWEGIE

22. On or about September 17, 2020, the CHS met with OSEMWEGIE at Five Guys in Peabody, Massachusetts. This meeting, arranged through the same WhatsApp phone number that CW-1 had provided for OSEMWEGIE, was audio and video recorded and surveilled by FBI agents. During the Peabody meeting, OSEMWEGIE agreed to transfer the CHS's fraud proceeds. In substance and in part, the meeting included the following statements:

[4] Verbal conversations between the CHS and OSEMWEGIE occurred primarily in English. For the most part the substance of the conversations in comprehensible in English, with some Nigerian Pidgin inserted into greetings or other comments.

a. OSEMWEGIE said he had over ten people who give him money, and that he would be buying a $25,000 car the next day.

b. OSEMWEGIE said he paid out Naira right away for money that people give him.

c. The CHS discussed using Bitcoin as a way to avoid having fraud traced to them and also to avoid questions from Nigerian law enforcement due to sending too much money to Nigeria. OSEMWEGIE told the CHS that he, OSWEMEGIE, has had that problem in the past when he was doing 30-40 million.[5]

d. OSEMWEGIE told the CHS he was concerned when CW-1 had called (to introduce the CHS) because OSEMWEGIE had heard about CW-1's situation and did not want to be associated. OSEMWEGIE told CW-1 that he was concerned because he, OSEMWEGIE, used to "buy money" from CW-1, adding that it was a lot of money.

e. The CHS told OSEMWEGIE that the CHS's money came from unemployment and Payroll Protection scams. The CHS told OSEMWEGIE he wanted to move $13,000 to either Bitcoin or to an account in Canada. In the CHS's presence, OSEMWEGIE called a friend to discuss sending Bitcoin.

f. OSEMWEGIE and the CHS negotiated over the fee. Ultimately, OSEMWEGIE agreed to a 20 percent fee, noting that he would have to give

[5] It was not clear if OSEMWEGIE was referring to dollars or naira, but it appears more consistent with the volume of business described above that it was naira. As of August 13, 2021, 30-40 million naira would be approximately $72,000 to $97,000.

the friend he had called some of the proceeds for assistance with sending the Bitcoin.

g. The CHS told OSEMWEGIE that more funds would be coming in soon and that the CHS would like to continue to use OSEMWEGIE to move money.

23. At the conclusion of the meeting, the CHS gave OSEMWEGIE an envelope that contained $13,000 in cash (which the FBI had given the CHS).

OSEMWEGIE Wired the $13,000 the CHS Provided to a Canadian Account

24. Later in the day on or about September 17, 2020, OSEMWEGIE contacted the CHS and, in a change to the plan of converting the $13,000 to Bitcoin that he and the CHS had discussed, stated that OSEMWEGIE had decided to send the money to an account the CHS controlled account in Canada. OSEMWEGIE also increased his percentage to 30 percent. At the FBI's direction, the CHS provided OSEMWEGIE with account information for an FBI-controlled account in Canada to receive the money.

25. TD Bank records indicate that on or about September 18, 2020, OSEMWEGIE deposited $7,990 in cash into the Ejad Auto Sales account there. Prior to this deposit the account would have not been able to fund the wire discussed in the following paragraph.

26. On or about September 21, 2020, OSEMWEGIE sent the CHS a screenshot showing the transmission of a $10,000 wire from the Ejad Auto Sales TD Bank account to the account in Canada for which the CHS has provided the information. OSEMWEGIE followed the picture with a message that read, "The money has been paid for the 2012 Lexus RX350…. PLS confirm." On the outgoing wire transfer form from TD Bank, OSEMWEGIE listed his relationship to the beneficiary as "car dealer", and the reference as "Payment For 2012 Lexus

Rx350", as depicted below:

TD Bank

CUSTOMER COPY

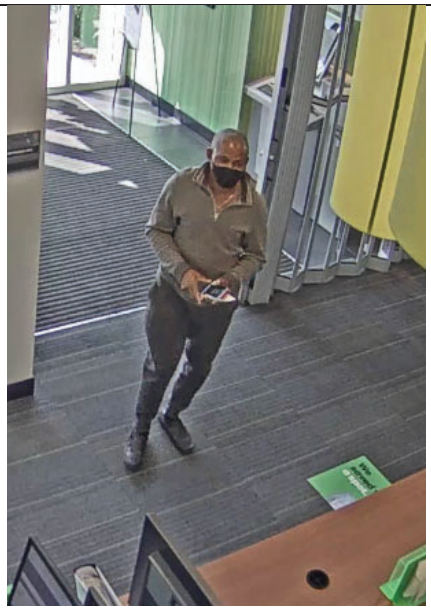
OUTGOING WIRE TRANSFER FORM

Reference #: 09212012143168

Bank: 003 *Branch Number:* 1355

Foreign Amount & Currency Type: 12,931.59 CAD	Rate: 0.773300	USD Amt: $10,000.00	Fees: $50.00
TRANSFER REQUEST DATE: 09/21/2020		Total: $10,050.00	
Relationship to Beneficiary: car dealer	Source of Wire: International Wire - In Person		
Purpose of Wire: Purchase Inventory	Purpose: Additional Info:		
Beneficiary Name: [redacted]	Beneficiary Address 1: [redacted]		
Beneficiary Address 2:	City: Ottawa Country: Canada		
Beneficiary Account/IBAN or CLABE Number: [redacted]	Other ID:		
Beneficiary Bank: [redacted]	Beneficiary Bank Address 1: 1145 Wellington St		
Beneficiary Bank Address 2:	City: Ottawa Country: Canada		
Beneficiary Bank Code: [redacted]	Reference: Payment For 2012 Lexus Rx350		
Intermediary Bank:	Intermediary Bank Code:		
Correspondent Bank:	ABA: TDOMCATTTOR		
Name of our Customer: Ejad Auto Sales	Customer Phone:		
Address: 736 CUMMINS HWY MATTAPAN, MA 02126-3246	Account Number to be charged: 8258375150		

27. Surveillance acquired from TD Bank shows OSEMWEGIE conducting a deposit into the Ejad Auto Sales account on or about September 18, 2020, and sending the wire to the Canadian FBI account on or about September 21, 2020:

	
Sept. 18, 2020 $7,990 deposit at a TD Bank in Billerica, Massachusetts	Sept. 21, 2020 $10,000 wire at TD Bank Roslindale, Massachusetts

28. On or about September 28, 2020, the CHS and OSEMWEGIE exchanged the following WhatsApp messages between the CHS's FBI-provided telephone and the number that CW-1 and the CHS had used to communicate with OSWEMWEGIE's, 617-997-7687.

Sender	Time	Message
CHS	10:50 AM	I am still waiting and will call you once I get the money
CHS	11:15 AM	I am at work
OSEMWEGIE	11:16 AM	Tools not money
CHS	11:16 AM	I can not be able to pick a call
CHS	11:16 AM	Okay

Ejad Auto Sales Receives Money From Macpherson Osemwegie

29. On or about March 25, 2021, the FBI arrested Macpherson Osemwegie, a/k/a Benedict LeJeune, a/k/a George Wood, a/k/a Desmond Barnabas, a/k/a Philip Weah,[6] for violating 18 U.S.C. § 1349 (bank and wire fraud conspiracy). *See United States v. Macpherson Osemwegie*, 21-mj-4101-DHH.

30. On or about July 21, 2021, the United States filed an Information and plea agreement as to the same charge against Macpherson Osemwegie. A Rule 11 hearing is scheduled before the Honorable Denise J. Casper, United States District Judge, on August 26, 2021. *See* 21-CR-10219-DJC. According to the allegations in the Information to which Macpherson has agreed to plead guilty, Macpherson was involved in a similar network as CW-1 and was receiving proceeds of various fraud scams.

[6] Although they have the same last name, there is no known family relationship between Augustin Osemwegie and Macpherson Osemwegie.

31. On or about August 13, 2020, two $1,000 United States Postal Money Orders from Macpherson Osemwegie were deposited into the Ejad Auto Sales account at Chase Bank, which is described above in paragraph 11.

PROBABLE CAUSE TO BELIEVE THAT THE SUBJECT PREMISES CONTAIN EVIDENCE, FRUITS, AND INSTRUMENTALITIES

32. There is also probable cause to believe, for the reasons stated above and below, that OSEMWEGIE's residence, the SUBJECT PREMISES, contains fruits, evidence, and instrumentalities of the TARGET OFFENSES.

33. On September 4, 2020, during a call between the CHS and OSEMWEGIE, OSEMWEGIE told the CHS that he did not want to text his address, but he lives at "104 Thacher St." (*i.e.*, the SUBJECT PREMISES).

34. In addition, on multiple occasions between October 13, 2020 and February 18, 2021, surveillance observed either OSEMWEGIE or vehicles registered to him at the SUBJECT PREMISES. OSEMWEGIE is believed to live at the SUBJECT PREMISIES with his spouse and several children.

35. CW-1 identified the SUBJECT PREMISES as OSEMWEGIE's residence.

36. Based on my training and experience investigating financial crimes, I know that locations occupied by a target often 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.

37. I am also aware, based on my training and experience, that individuals engaged in money laundering and financial frauds retain records of accounts they have opened in furtherance of those frauds. Among other reasons, participants in a fraud do not always appreciate the

incriminating nature of records that banks provide in the ordinary course of business. Although subjects may make efforts to destroy or eliminate such records, it is reasonable to believe that some are retained intentionally, or by accident. Participants in a fraud also need to be able to document the proceeds of the fraud to show a scheme's net proceeds and the resulting amounts due to coconspirators. As with the false identifications, bank accounts (and the records they generate) can be used over long periods of time in connection with several financial transactions. In addition, individuals who perpetrate fraudulent schemes and/or launder the proceeds also keep ledgers of proceeds, similar to drug traffickers, that often are found where they reside.

38. Finally, I know based on my training and experience as an investigator, that even if they fail to keep written or electronic records of their activities, individuals involved in financial fraud and money laundering activities are unlikely to destroy clothing that they wore when conducting bank transactions.

39. Accordingly, there is probable cause to believe that the SUBJECT PREMISES, which is OSEMWEGIE's residence, will contain evidence of the TARGET OFFENSES, including without limitation clothing matching the clothing worn in surveillance images and videos; bank account opening documents, monthly statements, debit cards, ATM receipts, and other banking materials related to OSEMWEGIE, Ejad Auto Sales, and the TARGET OFFENSES; ledgers and passwords associated with the accounts; computers and telephones used to communicate with co-conspirators; and cash.

40. As discussed below, I also expect that cellular phones and/or computers owned and used by OSEMWEGIE will contain evidence of the TARGET OFFENSES, and in my experience, cellular phones and computers are typically found where targets reside. As described above, OSEMWEGIE used a cellular telephone to communicate with CW-1 and used a cellular telephone

to communicate with the CHS in September 2020 to arrange and confirm the transfer of what he was told were the proceeds of fraud to Canada. In addition, on or about June 30, 2021, according to CW-1, OSEMWEGIE called CW-1 from telephone number (617) 997-7687 and asked if CW-1 had any money to move. Further, targets tend not to discard computers and cellular phones in my experience, and even if they do, targets frequently "backup" their computers and cellular phones to new devices, the cloud, or external hard drives, and they keep those records for the reasons stated above.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

41. 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 e-mail, instant messages, and updates to online social-networking websites; drafting letters; keeping their calendars; arranging for travel; storing pictures; researching topics of interest; buying and selling items online; and accessing their bank, financial, investment, utility, and other accounts online.

42. 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 of communications and evidence that reveals or suggests who possessed or used the device.

43. I am aware of a report from the United States Census Bureau that shows that in 2016, among all households nationally, 89 percent had a computer, which includes smartphones, and 81 percent had a broadband Internet subscription. Specifically, in 2016, when the use of smartphone ownership was measured separately for the first time, 76 percent of households had a smartphone and 58 percent of households had a tablet, and 77 percent of households had a desktop or laptop computer. Further, according to the Pew Research Center, as of 2019, 96 percent of adult Americans own a cellphone, and 81 percent own a cellphone with significant computing capability (a "smartphone"). The percentage of adults that own a smartphone is even higher among younger demographic groups: 96 percent of 18-29 year olds, 92 percent of 30-49 year olds, and 79 percent of 50-64 year olds owned smartphones in 2019.

44. 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 the dates files were created and the sequence in which they were created, although this information can later be falsified.

f. 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 United States 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 crime 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).

g. 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.

h. 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.

i. 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.

45. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order 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 — storage media such as hard disks, flash drives, CDs, and DVDs can store 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 on-site.

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.

46. The premises may contain computer equipment whose use in the crime(s) 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 in order 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.

47. 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. 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.

UNLOCKING A DEVICE USING BIOMETRIC FEATURES

48. 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.

49. 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 5 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 (5) five unsuccessful attempts to unlock the device via Touch ID are made.

50. The passcode that would unlock OSEMWEGIOE's device, if it is found during the search of the SUBJECT PREMISES, is not currently known to law enforcement. Thus, it may be useful to press OSEMWEGIE's finger(s) to any device found during the search of the Subject Premises to the device's fingerprint sensor or to hold the device up to OSEMWEGIE's face 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 that device for the purpose of executing the search authorized by this warrant.

51. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of OSEMWEGIE to the sensor of the device or place the device in front of his face for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

CONCLUSION

52. Based on the information described above, I have probable cause to believe that OSEMWEGIE committed conspiracy to commit bank and wire fraud, in violation of 18 U.S.C. § 1349, and that evidence, fruits, and instrumentalities of that crime, and the other TARGET OFFENSES set forth above, as described in Attachment B to the proposed warrant, are contained within the SUBJECT PREMISES as described in Attachment A to the proposed search warrant.

Michael Livingood/DHH

MICHAEL LIVINGOOD
Special Agent, Federal Bureau of Investigation

Subscribed and sworn to by telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 25th day of August 2021.

David H. Hennessy

Hon. David H. Hennessy
United States Magistrate Judge