AFFIDAVIT OF SPECIAL AGENT MICHAEL LIVINGOOD IN SUPPORT OF AN APPLICATION FOR A COMPLAINT AND SEARCH WARRANTS

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 the following individuals (collectively, the "TARGET SUBJECTS") with conspiracy to commit bank and wire fraud, in violation of 18 U.S.C. § 1349:

      (1) MACPHERSON OSEMWEGIE, also known as Desmond Barnabas, also known as Benedict Lejeune, also known as George Wood, and also known as Philip Weah ("MACPHERSON OSEMWEGIE");

      (2) OSAKPAMWAN HENRY OMORUYI, also known as Clifford Bernard ("HENRY OMORUYI"); and

      (3) OSARETIN GODSPOWER OMORUYI, also known as Samuel Kwamen ("OSARETIN OMORUYI"),

(b) search warrants for the following premises (collectively, the "SUBJECT PREMISES"):

(1) the residence of MACPHERSON OSEMWEGIE, located at 7 Lincoln St., Apt. 4, Hyde Park, Massachusetts ("SUBJECT PREMISES 1"), as described in Attachment A1;

(2) the residence of OSAKPAMWAN HENRY OMORUYI and OSARETIN OMORUYI, located at 20 Bailey Court, Apt. E, Canton, Massachusetts ("SUBJECT PREMISES 2"), as described in Attachment A2;

(3) Storage Unit 1017, located at Prime Storage, 1641 Hyde Park Ave., Hyde Park, Massachusetts, and registered to OSAKPAMWAN HENRY OMORUYI ("SUBJECT PREMISES 3"), as described in Attachment A3,

(c) search warrants for the following vehicles (collectively, the "SUBJECT VEHICLES"):

(1) a 2005 Ford F-350 truck, bearing Massachusetts registration number 1AMK78, Vehicle Identification Number ("VIN"): 1FTWW31P85EC95848, registered to MACPHERSON OSEMWEGIE ("SUBJECT VEHICLE 1"), as described in Attachment A4;

(2) a 2016 Toyota Corolla automobile, bearing Massachusetts registration number 7PM222, VIN: 2T1BURHE5GC673951, registered to OSAKPAMWAN HENRY OMORUYI ("SUBJECT VEHICLE 2"), as described in Attachment A5; and

(3) a 2013 Toyota Avalon automobile, bearing Massachusetts registration number 7XCC70, VIN: 4T1BK1EB8DU066017, registered to OSARETIN OMORUYI ("SUBJECT VEHICLE 3"), as described in Attachment A6,

because there is probable cause to believe that the SUBJECT PREMISES and the SUBJECT VEHICLES contain evidence, fruits and instrumentalities of violations of federal law, including Title 18, United States Code, Sections 371 (conspiracy), 1014 (false statements to a bank), 1028A (aggravated identity theft), 1343 (wire fraud), 1344 (bank fraud), 1349 (attempt and conspiracy), 1543 (forgery or false use of a passport), 1956 and 1957 (money laundering and conspiracy to

commit money laundering) (collectively, the "TARGET OFFENSES"), as described in Attachment B.

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 warrants and does not set forth all my knowledge about this matter.

PROBABLE CAUSE THAT FEDERAL CRIMES WERE COMMITTED

4. As set forth below, there is probable cause to believe that, between at least 2017 and the present, MACPHERSON OSEMWEGIE, OSAKPAMWAN HENRY OMORUYI, and OSARETIN GODSPOWER OMORUYI, together with others known and unknown, engaged in a conspiracy to commit bank and wire fraud, in violation of Title 18, United States Code, Section 1349, as well as other crimes, through a series of scams—including romance, pandemic unemployment insurance, and other schemes—designed to defraud victims into sending money to accounts controlled by the TARGET SUBJECTS in their own names and other names they used.

5. To carry out their fraud scheme, the TARGET SUBJECTS used false foreign passports, in the names of others but with the TARGET SUBJECTS' own photos, to open multiple bank accounts, and directed victims to send money to those accounts. The TARGET SUBJECTS, together with others known and unknown, then withdrew the victims' money from various bank branches and ATM machines, often making multiple withdrawals in a single day. The TARGET SUBJECTS also used accounts in the names of others to receive and withdraw victims' funds.

6. The affected banks—including Bank of America, N.A., J.P. Morgan Chase, N.A., Citizen's Bank, N.A., Santander Bank, N.A., TD Bank N.A., Eastern Bank, Blue Hills Bank/ Rockland Trust Bank, are all financial institutions within the meaning of 18 U.S.C. § 2.

MACPHERSON OSEMWEGIE

7. On or about December 20, 2020, the FBI received a tip from an individual who used an alias. The caller stated that MACPHERSON OSEMWEGIE was involved in credit card and unemployment fraud and provided the address of SUBJECT PREMISES 1, and MACPHERSON OSEMWEGIE's current phone number, (617) 291-7455, during the call.

8. I have interviewed this caller, who reported that the caller had heard from multiple friends that MACPHERSON OSEMWEGIE was involved in various frauds, including unemployment fraud; that MACPHERSON OSEMWEGIE's friend, HENRY OMORUYI, and other friends, were involved in the alleged frauds; that the caller had personally observed numerous credit cards, gift cards, and a false passport inside MACPHERSON OSEMWEGIE's residence at SUBJECT PREMISES 1; and that MACPHERSON OSEMWEGIE sent some of the fraud proceeds to family members in Nigeria, and used some of the proceeds to buy a house in Nigeria.

9. A review of bank records and surveillance photos indicates that MACPHERSON OSEMWEGIE is associated with at least 16 different bank accounts, using four different fake passports, with four different identities.[1] The accounts and relevant information are listed below:

[1] Some entries in the Desmond Barnabas accounts were also inverted and listed in the name of Barnabas Desmond.

	Name Used	Financial Institution	Date Opened	Phone # Listed
1	Benedict LeJeune	TD Bank	06/16/2017	781-202-6264 857-701-9464
2	Benedict LeJeune	Bank of America	07/26/2017	857-701-9464
3	Benedict LeJeune	Santander Bank	02/20/2018	**617-792-4556 (# also used by Wood)**
4	George Wood	Blue Hills Bank/ Rockland Trust Bank	04/10/2018	**617-792-4556 (# also used by LeJeune)**
5	George Wood	Eastern Bank	04/11/2018	857-399-7373
6	George Wood	Santander Bank	04/11/2018	857-399-7373
7	Desmond Barnabas	Citizen's Bank	12/22/2018	617-991-5232
8	Desmond Barnabas	TD Bank	12/22/2018	617-991-5232
9	Desmond Barnabas	Bank of America	03/22/2019	617-991-5232
10	Desmond Barnabas	J.P. Morgan Chase Bank	03/29/2019	617-991-5232
11	Desmond Barnabas	Santander Bank	12/06/2019	617-991-5232
12	Philip Weah	Citizens Bank	03/09/2019	617-953-2565
13	Philip Weah	TD Bank	10/17/2019	617-953-2565
14	Philip Weah	JP Morgan Chase Bank	02/11/2020	617-953-2565
15	Philip Weah	Bank of America	02/12/2020	617-953-2565
16	Philip Weah	Rockland Trust Bank	02/13/2020	617-953-2565

10. I have reviewed bank surveillance photos depicting an individual who accessed the above-listed accounts opened in the names of Desmond Barnabas, Benedict Lejeune, George Wood, and Philip Weah. The photos all appear to resemble the Massachusetts driver's license photo of MACPHERSON OSEMWEGIE.[2] Some of these photos are set forth below:

Figure 1.1: George Wood Attempted withdrawal – Eastern Bank ($8,300 on 05/30/2018 – Jamaica Plain, MA)

Figure 1.3: MACPHERSON OSEMWEGIE's Massachusetts Driver's License Photo

Figure 1.2: Desmond Barnabas TD Bank withdrawal (02/27/2019, $2,600 – Quincy, MA)

Figure 1.4: Benedict Lejeune Bank of America withdrawal (04/24/2018, $5,900 – Dorchester, MA)

[2] Based on a review of bank surveillance images and discussions with bank investigators, I believe that other individuals may also have engaged in transactions in the Wood Eastern Bank account. I know from my training and experience and that these individuals may be "runners", or persons employed by or working as co-conspirators with the account owner.

Figure 1.5: Philip Weah Rockland Trust deposit (03/03/2020, Hyde Park, MA)

11. I have conducted and reviewed surveillance at SUBJECT PREMISES 1 and 3 and have observed MACPHERSON OSEMWEGIE coming to and from these premises, driving SUBJECT VEHICLE 1, and traveling various places. The person I observed at SUBJECT PREMISES 1 and 3 and in SUBJECT VEHICLE 1 resembles the person in the bank surveillance photos depicted above.

12. The accounts of George Wood and Benedict Lejeune both listed a common phone number (617) 792-4556 in the account opening documents. The phone number listed for the bank accounts of Philip Weah, (617) 953-2565, was also provided by HENRY OMORUYI as an alternate phone number in connection with the renting of SUBJECT PREMISES 3, as described further below.[3]

[3] In addition, I am aware that the telephone of another individual, Kofi Osei ("Osei"), also known as Paul Proia, Kenneth Buck, and Jeffrey Anashe—which was searched pursuant to a Court-authorized search warrant—contained messages between Osei and MACPHERSON OSEMWEGIE on his personal phone ((617) 291-7455) concerning the accounts described above. On or about March 21, 2018, MACPHERSON OSEMWEGIE sent Osei a message containing the name Benedict Lejeune and the bank account number for the account opened in Lejeune's name at Bank of America. On or about December 12, 2018, MACPHERSON OSEMWEGIE sent Osei a message containing the name Barnabas Desmond and the address 51 Lincoln St., Apt, 2, Hyde Park, Massachusetts. Osei was recently indicted in the United States District Court for the District of Massachusetts for making false statements to a bank, wire fraud, and money laundering, in violation of Title 18, United States Code, Sections 1014, 1343, and 1956, respectively.

13. On or about March 3, 2021, an FBI surveillance team observed MACPHERSON OSEMWEGIE driving SUBJECT VEHICLE 1 and traveling to five separate Walmart locations in Walpole, Brockton, Avon, Weymouth, and Quincy, Massachusetts. After visiting the first Walmart location, MACPHERSON OSEMWEGIE also stopped briefly at SUBJECT PREMISES 2. Shortly after MACPHERSON OSEMWEGIE left SUBJECT PREMISES 2, HENRY OMORUYI left the residence as well. During the evening, MACPHERSON OSEMWEGIE was driven to a sixth Walmart by HENRY OMORUYI in SUBJECT VEHICLE 2. According to Walmart records, MACPHERSON OSEMWEGIE used multiple Green Dot cards to conduct cash withdrawals totaling $15,150 in the same day. According to records received from Green Dot, the funds on those cards came from unemployment payments in the names of others.

14. The records of the bank accounts listed above demonstrate that they were used to receive and launder the proceeds of various frauds. Set forth below are a few examples:

Victim 1 - Virginia Beach, Virginia

15. On or about October 31, 2018, the Benedict Lejeune Santander Bank account received a $1,250 wire from Victim 1, a 68-year-old woman who resides in Virginia Beach, Virginia. The funds were quickly withdrawn in cash over the next day or two.

16. I have interviewed Victim 1, who told me that she had met a man online named David Smith. Smith told Victim 1 that he was an officer in the United States Army stationed overseas. According to Victim 1, Smith requested money for, among other things, his daughter's education, his travel, and his medical expenses. Victim 1 said that, in order to provide the funds Smith requested, she sold her house and depleted her retirement savings.

Victim 2 – Idaho Falls, Idaho

17. On or about April 3, 2018, the Lejeune Santander Bank account received a $71,200 wire from Victim 2, a 62-year-old woman who resides in Idaho Falls, Idaho. The funds were quickly withdrawn over the next six days, as follows:

Date	Activity	Amount
04/03/2018	Incoming Wire Transfer – [Victim 2 Name]	$71,200
04/04/2018	Cash Withdrawal	- $9,500
04/04/2018	Cash Withdrawal	- $7,000
04/05/2018	Cashier's Check Purchase – Benedict Lejeune	-$25,000
04/06/2018	Cash Withdrawal	-$9,500
04/09/2018	Cash Withdrawal	-$9,500
04/09/2018	Cash Withdrawal	-$9,000
04/12/2018	Cash Withdrawal	-$800
04/16/2018	Cash Withdrawal	-$200
Point of sale transactions between 04/04/2018 and 04/12/2018 totaled an additional $609		

18. On or about April 5, 2018—the same day that a cashier's check in the amount of $25,000 was purchased from the Lejeune Santander account, a cashier's check in the same amount was deposited into the Lejeune Bank of America account. These funds were then withdrawn in cash over the next ten days.

19. On or about May 13, 2019, Victim 2 was interviewed by FBI agents and reported that in the wake of her husband's death in an accident in April 2009, she had received life insurance proceeds of approximately $1 million. According to Victim 2, in or about 2014, she began sending

a total of approximately $500,000 to various intermediaries and third parties at the request of individuals she met on social media and dating websites, who also instructed her to open corporations and affiliated bank accounts. Victim 2 said she sent money via Western Union, domestic and international wires, including the $71,200 wire to Benedict Lejeune.

Victim 3 - Portland Oregon

20. On or about May 12, 2018 and May 25, 2018, Victim 3, an 81-year-old woman who resides in Portland, Oregon, wired $2,000 and $20,000, respectively, to the Wood Eastern Bank account. According to a complaint filed by Victim 3's daughter, Victim 3 was the victim of a romance scam over a period of three years and sent the funds at the direction of her purported boyfriend.

21. After the arrival of Victim 3's funds into the Wood Eastern Bank account, approximately $2,600 was withdrawn from the account via cash and point-of-sale purchases. Eastern Bank subsequently froze the remaining funds in the account and returned about $19,381 to Victim 3.

Overview of Activity in Accounts Associated with MACPHERSON OSEMWEGIE

22. A review of the Wood, Barnabas, LeJeune, and Weah bank accounts shows similar conduct to that described above, including large deposits from individuals and businesses followed by immediate large cash withdrawals, as well as wire recalls due to alleged fraud. TD Bank restricted the Barnabas account due to a wire recall and contacted the individual identified as Barnabas to inquire about the conduct in the account. "Barnabas"—whom I believe to be MACPHERESON OSEMWGIE, based on the evidence set forth above—told TD Bank investigators, in sum and substance, that he sells cars and ships them internationally. TD Bank

investigators asked Barnabas to provide documentation to support these claims, but Barnabas did not do so.

23. A review of these accounts, all of which are associated with MACPHERSON OSEMWEGIE, as set forth above, shows estimated victim losses totaling approximately $690,000.

HENRY OMORUYI

24. On or about January 7, 2021, I conducted surveillance at SUBJECT PREMISES 1. I observed an individual who appeared to be MACPHERSON OSEMWEGIE enter a car that pulled up outside the residence. I followed the car to a storage facility, Prime Storage, located at 1641 Hyde Park Ave, Hyde Park, MA, 02136.

25. I have reviewed records indicating that HENRY OMORUYI has leased a storage unit at the Prime Storage facility, since on or about March 28, 2020, and upgraded to a larger unit, SUBJECT PREMISES 3, on or about May 7, 2020. On both occasions, HENRY OMORUYI provided a home address of 1110 River St., Hyde Park, MA, and a telephone number of 617-602-6560. I have learned that this phone number was used in March 2020 to open bank accounts in the name of "Clifford Bernard", using what appears to be a fraudulent passport, as described below. HENRY OMORUYI also provided Prime Storage an alternative phone number of 617-953-2565, which, as noted above, was used to open bank accounts in the name of Philip Weah. The River Street address is a residential building with three apartments.

26. Logs for SUBJECT PREMISES 3 show that the storage unit is accessed frequently. For example, in December 2020, the facility was accessed 31 times, in some instances multiple times on the same day. Surveillance images for the period from November 24, 2020 to January 7, 2021 show vehicles registered to MACPHERSON OSEMWEGIE and HENRY OMORUYI regularly arriving at Prime Storage, and individuals matching the descriptions of MACPHERSON

OSEMWEGIE and HENRY OMORUYI accessing the storage facility. SUBJECT VEHICLE 1 appears in the surveillance images approximately 10 times and SUBJECT VEHICLE 2 appears on the surveillance images approximately 6 times. MACPHERSON OSEMWEGIE and HENRY OMORUYI also visited SUBJECT PREMISES 3 in other vehicles, registered in the names of others, as well as in rental vehicles.

27. During some of the visits to SUBJECT PREMISES 3, the individuals accessing the unit can be seen carrying documents or records, and on one occasion, luggage. On multiple occasions, the individuals can be seen accessing their phones. I know from my training and experience that individuals using multiple identities and bank accounts to commit fraud frequently rely on electronic communications, notes, and records to keep track of which identities and documents they are using on a given day.

28. In or about March and April 2020, a person purporting to be Clifford Bernard opened accounts at TD Bank and Santander Bank, as set forth in the table below:

Name on Passport and Acct.	**Financial Institution**	**Date Opened**	**Phone #**	**Address**
Clifford Bernard	TD Bank	03/17/2020	617-602-6560	1110 River Street Hyde Park, MA
Clifford Bernard	Santander Bank	04/30/2020	617-602-6560	1110 River Street Hyde Park, MA

29. In the account applications, the person claimed not to be a U.S. citizen. The accounts were opened using a Ghanaian passport (PP # G0324745), with a photo that appears to be HENRY OMORUYI. I have searched United States Department of Homeland Security ("DHS") records, which lists all entries by foreign citizens, and was unable to locate travel or visa records for this passport.

30. I reviewed the Bernard accounts and learned that they were used to receive and launder the proceeds of various frauds, examples of which are described below.

Victim 4 - Louisville, Kentucky

31. On or about February 26, 2020, I interviewed Victim 4, a 65-year-old woman who resides in Louisville, Kentucky, who reported that in or around April 2020, she received a Facebook "friend" request from a man name Larry Midkiff Richard ("Richard"). Richard told Victim 4 that he was in the United States Army, serving in Iraq. Victim 4 began texting with Richard, and they developed romantic ties. Victim 4 never met Richard in person.

32. According to Victim 4, Richard claimed that he needed to pay money to get out of military service, so that he could come and be with her. Richard asked Victim 4 to provide the money. Richard claimed that he had rescued a prince and had money at his disposal to pay her back later.

33. At Richard's direction, Victim 4 sent money to Clifford Bernard via multiple cashier's checks. Victim 4 sent the checks via FedEx to an unknown address in Hyde Park, Massachusetts. Victim 4 understood Bernard to be Richard's commanding officer who was receiving the funds needed for his release from military service.

34. On or about July 13, 2020, a cashier's check obtained by Victim 4 was deposited into the Bernard Santander account and used to fund cash withdrawals and the purchase of a $20,000 cashier's check payable to HENRY OMORUYI, as follows:

Date	Activity	Amount
07/13/2020	Cashier's Check Deposit-[Victim 4 Name]	$30,000
07/14/2020	Cash Withdrawal	- $200
07/14/2020	Cash Withdrawal	- $800
07/14/2020	Cash Withdrawal	-$800
07/14/2020	Cash Withdrawal	-$4,200
07/15/2020	Cashier's Check Purchase – Henry Omoruyi	-$20,000
07/16/2020	Cash Withdrawal	-$1,800
07/16/2020	Cash Withdrawal	-$1,800

35. Victim 4 lost approximately $50,000 as part of the scam.

Victim 5 - Englewood, Ohio

36. On or about February 24, 2021, I interviewed Victim 5, a 60-year-old woman who resides in Englewood, Ohio, who reported that she met a man named Scott Midkiff sometime around the beginning of January 2020. Midkiff sent Victim 5 a Facebook friend request and they began chatting using WhatsApp and Google Hangouts. Midkiff claimed to be in the United States military and stationed in Afghanistan.

37. Shortly after Victim 5 began chatting with Midkiff, he began asking her for money. According to Victim 5, Midkiff stated that he needed the funds to be released from military service and to fund his travel back to the United States. Midkiff told Victim 5 that after he returned to the United States, he would move to be with her, and repay her all the money she provided to him.

38. Victim 5 began sending money at the direction of Midkiff. Victim 5 sent money to various individuals via wire transfers and cashier's checks. Victim 5 stated that Midkiff always came up with another reason to ask for money. At one point, Midkiff claimed to be in jail, and

needed money to be released. Victim 5 stated that she refinanced her home to provide funds to Midkiff.

39. On or about the dates set forth below, pursuant to Midkiff's directions, Victim 5 sent cashier's checks payable to HENRY OMORUYI and Clifford Bernard:

Date	Payee on Cashier's Check	Amount	Means of Delivery	Location Sent to
1/28/2020	Henry Omoruyi	$27,500	Fedex	Hyde Park
2/10/2020	Henry Omoruyi	$14,000	Fedex	Henry Omoruyi, 11 Albermarble, Boston, MA
3/25/2020	Clifferd [sic] Bernard	$31,000	Fedex	Clifford Bernard, 1110 River St, Hyde Park, MA

40. On or about February 13, 2020, HENRY OMORUYI deposited a cashier check obtained by Victim 5 in the amount of $14,000 into a Rockland Trust Company account in the name of OSAKPAMWAN HENRY OMORUYI.[4]

41. Rockland Trust personnel questioned HENRY OMORUYI about the transaction. Among other things, OMORUYI claimed that he had known Victim 5 for over two years and had her phone number. Victim 5, however, reported that she had never met and did not know anyone by the name of HENRY OMORUYI.

42. Victim 5 eventually conducted reverse image searches on the internet and found that the photographs Midkiff had sent of himself belonged to someone else.

Fraudulent COVID Unemployment Payments Deposited in Clifford Bernard TD Bank Account

[4] The opening application for this account used the address 1110 River Street, Hyde Park, MA, which is the same address that HENRY OMORUYI used in the application to lease SUBJECT PREMISES 3.

Victim 6 - Millinocket, Maine

43. On or about May 29, 2020 the TD Bank account under the Clifford Bernard name received two ACH credits totaling $8,205 for COVID-related unemployment benefits. These funds were spent or removed in cash over three weeks following the deposits.

44. The Maine Department of Labor ("MDL") reported that two unemployment assistance payments based on an application purporting to be for Victim 6, a resident of Millinocket, Maine, were paid into the Clifford Bernard TD account.

45. United States Department of State Diplomatic Security Service ("DSS") investigators interviewed Victim 6, who stated, in sum and substance, that he had been notified by mail in or about April 2020 that he had been approved for unemployment assistance. At the time, Victim 6 was not unemployed, but worked as a nurse at Millinocket Regional Hospital, where he had been employed steadily for approximately 35 years. Victim 6 said he had not applied for unemployment since approximately 1975 and had not received any payments from MDL in 2020. Agents reviewed Victim 6's personal information and confirmed that the name, date of birth, Social Security number, previous employer, and home address used on the application all belonged to Victim 6. The Application for Pandemic Unemployment Insurance submitted using Victim 6's information incorrectly claimed that he was a physician who was laid off from the hospital in January of 2020.

Fraudulent Passports Shipped to Henry Omoruyi, 1110 River St.

46. On or about March 7, 2018, while inspecting incoming packages to the United States, a United States Customs and Border Protection Officer located a package that was manifested as "DOCUMENT 1 INT L PASSPORT DRIVERS LICENCE". The package was shipped via United Parcel Service from Benin City, Nigeria, and was address to HENRY

OMORUYI, 1110 River St., Hyde Park, MA. Upon inspection, the package was found to contain a Nigerian Passport and Driver's License in the name of William Graf. These documents were determined to be counterfeit and were seized. The photo on the fake passport appears to be HENRY OMORUYI.

OSARETIN OMORUYI

47. From a review of bank records, I have found that the address 1110 River St., Hyde Park, MA, was used between in or about 2019 and 2021 in connection with numerous other bank accounts, including two in the name of Philip Weah, noted above, and two in the name of Samuel Kwamen, which as set forth below, is associated with OSARETIN OMORUYI. I have searched DHS records, which lists all entries by foreign citizens, and was unable to locate travel or visa records for each of these passports. The chart below depicts various account openings using the 1110 River St. address:

Name	**Date of Birth**	**Passport Country**	**Banks Identified**	**Approximate Date of Use**
Philip Weah	05/07/1983	Sierra Leone (ER036195)	Bank of America, JP Morgan	02/13/2020 – 06/30/2020
Samuel Kwamen	07/07/1982	Ghana (G1064499)	TD Bank, Santander Bank	09/2020 – 01/2021
Matins Kelvin	01/10/1982	Nigeria (A05888362)	TD Bank	11/2020 – 01/2021
Ben Johnson	09/29/1984	Nigeria (A07313494)	TD Bank, JP Morgan, Citizen's Bank	08/2019 – 01/2021
Philip Belcher	12/02/1983	United Kingdom (486105259)	Citizens Bank	07/2020 – 10/2020

48. In bank applications to TD Bank and Santander Bank, a person purporting to be Samuel Kwamen claimed not be a U.S. citizen, and opened accounts using a Ghanaian passport (PP # G1064499), as set forth below:

Name on Passport and Bank Acct. #	**Financial Institution**	**Date Opened**	**Telephone**	**Address**
Samuel Kwamen	TD Bank	05/15/2020	908-265-9775	1110 River Street Hyde Park MA
Samuel Kwamen	Santander Bank	05/14/2020	908-265-9775	1110 River Street Hyde Park, MA

49. On or about June 10, 2020, surveillance images from TD Bank show that an individual operating a vehicle with Massachusetts license plate 9VG313 accessed the Samuel Kwamen account. At the time the images were recorded, the vehicle was registered to OSARETIN OMORUYI, who is known to the State Department to be the brother of HENRY OMORUYI. The Massachusetts driver's license photograph of OSARETIN OMORUYI appears to show the same individual who accessed the Samuel Kwamen accounts on the TD Bank surveillance on June 10, 2020, among other times.

Victim 7 - Blairsville, Pennsylvania

50. On March 10, 2021, I interviewed Victim 7, a 55-year-old woman who resides in Blairsville, Pennsylvania, who reported that she met a man named David Samadi on Facebook and had been communicating with Samadi for approximately four years. Victim 7 believed that Samadi was a doctor temporarily providing aid in Afghanistan. Samadi asked Victim 7 for financial assistance. On one occasion, Samadi also sent Victim 7 a $40,000 check, which Victim 7 deposited into her account. However, Victim 7's bank reported the check as fraudulent and did not credit her account. Samadi also caused more than $17,000 in Illinois unemployment benefits,

in the name of a third person, to be deposited into Victim 7's bank account. This credit was returned by the bank before anyone accessed it.

51. On or about June 9, 2020, at Samadi's direction, Victim 7 wired $2,000 to a TD Bank account in the name of Samuel Kwamen.

52. On or about June 10, 2020, an individual driving the car registered to OSARETIN OMORUYI and identified from bank surveillance photos as OSARETIN OMORUYI drove to the TD Bank window in Roslindale, Massachusetts and withdrew $1,940 in cash from the TD Bank account in the name of Samuel Kwamen.

Fraud on Small Business Administration Disaster Loan and Pandemic Unemployment Fraud

Victim 8 - Dehli, Iowa

53. On or about August 4, 2020 a TD Bank account opened in the name of Samuel Kwamen and believed to be controlled and/or accessed by OSARETIN OMORUYI received a $47,200 ACH credit from "SBAD Treasury 310".

54. Investigators at the U.S. Department of the Treasury and the Small Business Administration ("SBA") provided documentation showing that the credit was made pursuant to an SBA Disaster loan application by Victim 8.

55. DSS investigators interviewed Victim 8, a resident of Delhi, Iowa, who reported that on or about October 14, 2020, she began receiving notices from the SBA stating that payments on her SBA loan would begin in August 2021. Victim 8 had not applied for an SBA loan and did not own the business named in the loan application.

56. DSS agents confirmed that the personal information on the loan application, including name, address, date of birth, and social security number, matched that of Victim 8.

57. One of the documents in the SBA loan file in the name of Victim 8 notes that the name on the account that received the loan funds was Samuel Kwamen. The account number on the SBA document matches a TD Bank account in the name of Samuel Kwamen.

Additional False Identity Connected to OSARETIN OMORUYI and SUBJECT VEHICLE 3

58. From in or around March 2020 to in or about February 2021, a South African passport in the name of Bright Nelson (PP#A02765839), was used to open accounts at TD Bank, JP Morgan Chase, Citizens Bank, and Rockland Trust. I have searched DHS records and was unable to locate travel or visa records for this passport. These accounts were used to engage in similar conduct as the other accounts outlined herein. Surveillance photos from a TD Bank drive-up ATM in Roslindale, Massachusetts show that on or about December 9, 2020, an individual in SUBJECT VEHICLE 3 engaged in a transaction in the Bright Nelson TD Bank account. According to Massachusetts Department of Motor Vehicle records, SUBJECT VEHICLE 3 is registered to OSARETIN OMORUYI.

Transfers of Funds to Nigeria

59. Between on or about September 14, 2020 and on or about December 4, 2020, more than $100,000 in cash and money orders were deposited into an account in the name of HENRY OMORUYI at J.P. Morgan Chase Bank. The address HENRY OMORUYI provided in connection with the lease of SUBJECT PREMISES 3—1110 River Street—is listed in the address history in connection with this account. HENRY OMORUYI listed the following telephone number in the opening documents for this account: 617-596-4272.

60. During this time-period, more than $75,000 was wired from the J.P. Morgan Chase account to accounts at the First Bank Nigeria Limited in the names of HENRY OMORUYI and

OSARETIN OMORUYI, with approximately $54,000 to HENRY OMORUYI and $20,000 to OSARETIN OMORUYI.

61. Between on or about September 25, 2020 and on or about January 12, 2021, more than $134,000 in cash and money orders was deposited into a J.P. Morgan Chase account in the name of OSARETIN OMORUYI. OSARETIN OMORUYI listed the following telephone number in the opening documents for this account: 857-707-6400. During the same time-period, approximately $134,000 was wired from the account to accounts at the First Bank of Nigeria Limited in the name of OSARETIN OMORUYI.

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

62. I also have probable cause to believe that the SUBJECT PREMISES and the SUBJECT VEHICLES contain fruits, evidence, and instrumentalities of the TARGET OFFENSES, as set forth below.

THE SUBJECT PREMISES

63. 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.

64. I am also aware based on my training and experience that individuals engaged in money laundering often retain records related to stolen or falsified identities. This is because identities can be used more than once at different banks, as the TARGET SUBJECTS did in the investigation described above, opening several accounts under each identity. Even months after a fraud has been committed, identifications may be retained for use in new or ongoing frauds.

65. 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. When taken in whole, the subjects conducted hundreds of bank transactions, which produce receipts, and other records. 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

66. 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. Surveillance gathered from banks, Prime Storage, and law enforcement personnel, show the subjects wearing several distinctive articles of clothing, including sweatshirts and various stylized baseball hats, as well as jewelry such as necklaces, and bracelets.

67. Accordingly, I believe that it is likely that the SUBJECT PREMISES, which include the residences and a storage unit used by the TARGET SUBJECTS, will contain evidence

of the TARGET OFFENSES, including without limitation clothing matching clothing worn in surveillance images and videos; passports and other identification documents in the names of the TARGET SUBJECTS and the aliases they used to open bank accounts; bank account opening documents, monthly statements, debit cards, ATM receipts, and other banking materials related to the TARGET SUBJECTS and the TARGET OFFENSES; ledgers and passwords associated with the fraudulent accounts; computers and telephones used to communicate with co-conspirators and victims; and cash.

68. As discussed below, I also expect that cellular phones and/or computers owned and used by the TARGET SUBJECTS will contain evidence of the TARGET OFFENSES, and in my experience, cellular phones and computers are typically found where targets reside. 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, which may be found at the SUBJECT PREMISES.

SUBJECT PREMISES 1

69. Agents conducting surveillance have observed MACPHERSON OSEMWEGIE entering and exiting SUBJECT PREMISES 1, as well as parking his vehicle there overnight since at least December 2020. This address was also reported as MACPHERSON OSEMWEGIE's residence by the caller who reported MACPHERSON OSEMWEGIE's fraud activity in December 2020. On or about March 11, 2021, in response to subpoena, Eversource verified that MACPHERSON OSEMWEGIE is currently paying utility bills for this residence.

SUBJECT PREMISES 2

70. Surveillance teams have also observed HENRY OMORUYI and OSARETIN OMORUYI's vehicles parked at SUBJECT PREMISES 2 on a regular basis since February 2020, including late at night and early in the morning and have observed HENRY OMORUYI and OSARETIN OMORUYI leaving and arriving from these premises on various occasions.

SUBJECT PREMISES 3

71. As noted above, surveillance teams have observed MAPHERSON OSWEMWEGIE and HENRY OMORUYI arriving and departing from SUBJECT PREMISES 3 on numerous occasions. Also, the storage unit that is SUBJECT PREMISES 3 is leased in the name of HENRY OMORUYI.

THE SUBJECT VEHICLES

72. Based on my training, experience, and information obtained from other law enforcement agents, I understand that individuals who use fraudulent passports to access the proceeds of romance scams and other fraudulent schemes commonly store, among other things, fake identification documents, receipts, ledgers, and bank records inside their vehicles.

73. On numerous days between November 24, 2020 until March 3, 2021, surveillance from Prime Storage, various banks, and FBI surveillance teams have observed the SUBJECT VEHICLES being driven by MACPHERSON OSEMWEGIE, HENRY OMORUYI AND OSARETIN OMORUYI and traveling to banks, ATMs and SUBJECT PREMISE 3 at Prime Storage.

SUBJECT VEHICLE 1

74. As noted above, SUBJECT VEHICLE 1 is registered to MACPHERSON OSEMWEGIE. Between on or about November 24, 2020 and January 7, 2021, surveillance videos show that MACPHERSON OWEMWEGIE used SUBJECT VEHICLE 1 to visit SUBJECT PREMISES 3 at Prime Storage at least 10 separate times. On or about March 3, 2021, a surveillance team followed MACPHERSON OSEMWEGIE in SUBJECT VEHICLE 1 to 5 separate Walmart stores, where he was observed conducting cash withdrawals from the Walmart money centers and from ATMs. These cash withdrawals including obtaining cash from Green Dot debit cards. Records from Green Dot show that these funds come from multiple unemployment payments for different individuals.

SUBJECT VEHICLE 2

75. As noted above, SUBJECT VEHICLE 2 is registered to HENRY OMORUYI. Between on or about November 24, 2020 and January 7, 2021, HENRY OMORUYI and/or MACPHSERON OSEMWEGIE used SUBJECT VEHICLE 2 to visit SUBJECT PREMISES THREE at Prime Storage approximately 6 separate times. On or about March 3, 2021, HENRY OMORUYI used SUBJECT VEHICLE 2 to pick up MACPHERSON OSEMWEGIE and drive to the Walmart in Walpole, where MACPHERSON OSEMWEGIE again conducted multiple cash withdrawals.

SUBJECT VEHICLE 3

76. As noted above, SUBJECT VEHICLE 3 is registered to OSARETIN OMARUYI. On or about December 9, 2020, SUBJECT VEHICLE 3, was driven to a TD Bank branch in Roslindale, where a transaction was conducted under that identification of Bright Nelson. On or about January 22, 2021, a Postal Inspector observed SUBJECT VEHICLE 3 being driven from a

Canton Post Office by a person who obtained two postal money orders payable to OSARETIN OMORUYI in the amounts of $850 and $500.

SEIZURE OF COMPUTER EQUIPMENT AND DATA

77. 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.

78. 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.

79. 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. I know that Green Dot cards must be activated online before they are able to receive funds, and I know that at least some instances, the bank accounts referenced herein have been accessed via online login. I have also observed in surveillance photographs that the subjects herein, have utilized their phone when accessing the storage unit, and while conducting transactions at the bank.

80. 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.

81. 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.

82. 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.

83. 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

84. 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.

85. 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.

86. The passcode that would unlock the devices found during the search of the Target Premises is not currently known to law enforcement. Thus, it may be useful to press the finger(s) of the user(s) of the devices found during the search of the Target Premises 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.

87. 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).

88. For these reasons, I request that the Court authorize law enforcement to press the fingers (including thumbs) of one or more of the Defendants to the sensor of the devices or place the devices in front of their faces for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

CONCLUSION

89. Based on the information described above, I have probable cause to believe that the TARGET SUBJECTS 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 forth above, as described in Attachment B, are contained within the SUBJECT PREMISES and the SUBJECT VEHICLES, as described in Attachments A1-A6.

Sworn to, under the pains and penalties of perjury, by telephone in accordance with Federal Rule of Criminal Procedure 4.1 this 23rd day of March, 2021.

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 ___ day of March 2021.

Hon. David H. Hennessy
United States Magistrate Judge