

UNITED STATES DISTRICT COURT

for the
District of New Jersey**ORIGINAL FILED**

FEB 07 2020

WILLIAM T WALSH CLERK

United States of America

v.

Kayla Massa

Case No.

20-5518 (KMW)

Defendant(s)

CRIMINAL COMPLAINT

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

On or about the date(s) of See Attachment A in the county of _____ in the
_____ District of New Jersey, the defendant(s) violated:*Code Section*

18 U.S.C Section 1349

Description of Offenses

Conspiracy to committ bank fraud and wire fraud.

See Attachment A hereto.

This criminal complaint is based on these facts:

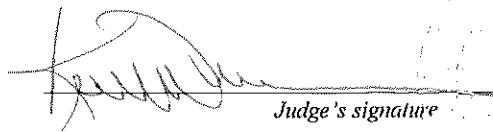
See Attachment B hereto.

☒ Continued on the attached sheet.*Complainant's signature*

Caitlin Plasecki, Postal Inspector

Printed name and title

Sworn to before me and signed in my presence.


Date: 02/07/2020City and state: Camden, New Jersey*Judge's signature*

Hon. Karen M. Williams, U.S. Magistrate Judge

Printed name and title

CONTENTS APPROVED

UNITED STATES ATTORNEY

By: 
ALISA SHVER
Assistant U.S. Attorney

Date: February 7, 2020

Attachment A

(Conspiracy to Commit Bank Fraud and Wire Fraud)

From on or about May 4, 2018 through in or about February, 2020, in the District of New Jersey, and elsewhere, the defendant,

KAYLA MASSA

did knowingly and intentionally conspire and agree with others, known and unknown, to devise a scheme and artifice to defraud financial institutions and the United States, and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice: (1) to cause to be transmitted by means of wire communications in interstate and foreign commerce, certain signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343; (2) to defraud a financial institution by means of materially false and fraudulent pretenses, representations, and promises, contrary to Title 18, United States Code, Section 1344, as described in Attachment B.

In violation of Title 18, United States Code Section 1349.

ATTACHMENT B

I, Caitlin Piasecki, having conducted an investigation and having spoken with other individuals, have knowledge of the following:

I am a United States Postal Inspector with the U.S. Postal Inspection Service ("USPIS"). I am aware of the facts contained in this Affidavit based upon my own investigation as well as information provided to me by other agents, law enforcement officers and witnesses. Because this Affidavit is submitted for the sole purpose of establishing probable cause to support the issuance of a Criminal Complaint, I have not included each and every fact known by the Government concerning this investigation. Rather, I have summarized sufficient facts to establish probable cause to believe that from in or about May 2018 through the present, in the District of New Jersey and elsewhere, the defendants, KAYLA MASSA ("MASSA"), JORDAN HERRIN ("HERRIN"), ERASMO FELICIANO ("FELICIANO"), WILLIAM LOGAN ("LOGAN") a/k/a "100k_nlb," DEZHON MCCRAE (MCCRAE) a/k/a "realycwoody," LEIRE LEIAN MASSA ("LEIRE") a/k/a "Onlyg0ldenLe," ALEX HAINES ("HAINES"), KEVIN MCDANIELS ("MCDANIELS") a/k/a "Chasesir100k" and JABREEL MARTIN ("MARTIN") a/k/a "1hunnit_mill," and ANDREW JOHNSON ("JOHNSON") a/k/a savage_santa, knowingly and intentionally conspiring with each other and others known and unknown to commit wire fraud contrary to Title 18, United States Code, Section 1343 and bank fraud contrary to Title 18 U.S.C. § 1344, in violation of Title 18, United States Code, Section 1349 (hereinafter the "Specified Federal Offenses"). Except as otherwise indicated, the actions, and statements of others identified in this Affidavit are reported in substance and in part.

I. Introduction

A. Defendants

1. Kayla Massa, (hereinafter “MASSA”), operates several social media accounts using SnapChat and Instagram, under the following names: “Kayg0ldi,” “Kay Kay,” and “theonlykayg0ldi.”
2. Jordan Herrin (hereinafter “HERRIN”), a resident of Berlin, was romantically involved with MASSA from approximately March 2017 through October 2018.
3. Erasmo Feliciano (hereinafter “FELICIANO”), a resident of Clementon and Sicklerville, New Jersey, is known by investigators to be in a romantic relationship with MASSA’s sister, Leire Leian Massa.
4. William Logan, (hereinafter “LOGAN”), a former resident of Glassboro, New Jersey, operates several social media accounts, to include Instagram and Facebook, under the following names: “Lamont Rose,” “100k_nlb,” “nlb_100k,” “nlb_93k, and “topopp_100k.”
5. Dezhon McCrae, (hereinafter “MCCRAE”), a resident of Penns Grove, New Jersey, operates several social media accounts, to include Instagram and Facebook, under the following names: “realcwoody” and “YC Woody.”
6. Leire Leian Massa (hereinafter “LEIRE”), MASSA’s sister, who is known by investigators to be in a romantic relationship with FELICIANO. LEIRE previously operated Instagram account, “g0ldenLe” and currently operates Instagram account “Onlyg0ldenLe” and Snapchat account “Le.”
7. Alex Haines (hereinafter “HAINES”), a resident of Woodbury, New Jersey, is an associate of LOGAN. HAINES worked at Woodbury Nissan from approximately September 2015 through November 2019.

8. Kevin McDaniels (hereinafter “MCDANIELS”), a resident of Sicklerville, New Jersey, is an associate of LOGAN and FELICIANO. MCDANIELS operates several social media accounts, include Instagram and Facebook, “chasesir100k” and “Kevo Back (Lil murda).”

9. Jabreel Martin (hereinafter “MARTIN”), a resident of Philadelphia, Pennsylvania, is an associate of LOGAN. MARTIN operates Instagram account “1hunit_mill.”

10. Andrew Johnson (hereinafter “JOHNSON”), a resident of Gloucester City, New Jersey, is an associate of FELICIANO. JOHNSON operates several social media accounts, to include Instagram and Facebook, under the following names, “Savage_Santa” and “Santaa_bagg.”

B. Entities and Terms

11. Instagram, also known as “IG” or “Insta,” is a photo and video-sharing social networking service and application owned by Facebook, Inc. The application, sometimes referred to as an “app,” allows users to upload photos and videos to the service, which can be edited with various filters, and organized with tags and location information, and are called “posts.” An account’s posts can be shared publicly or with pre-approved followers.

12. Users can browse other users’ content by tags and locations, and view trending content. Instagram “stories” are a feature that allow users to take photos, add effects and layers, and add them to a continual series of posts, also called a “story.” Images uploaded to a user’s story expire after 24 hours. Instagram account holders can change their displayed name, sometimes referred to as a “vanity name,” at any time on their account while maintaining their unique account identification number.

13. Snapchat, also known as “Snap” is a photo and video-sharing social networking service and application, sometimes referred to as an “app.” Snapchat enables users to create “snaps,” which are either photographs or videos captured in Snapchat, which can then be shared with the Snapchat users they add as “friends” on Snapchat. Once viewed, the “snap” will disappear and cannot be

retrieved. Snaps can also be posted to the user's "story," which is a compilation of "snaps" displayed in chronological order. "Stories" automatically delete 24 hours after being posted. Snap chat users can only view "snaps" with other Snapchat users on their "friends" list; "stories" can be viewed based on the users' settings to include everyone (all Snapchat users), "friends" or a custom list selected by the user. Users can communicate in Snapchat via "chat," a messaging platform within Snapchat.

The "chat" disappears after being viewed, unless settings are adjusted to allow "chats" to be remain for 24 hours. Snapchat users can edit settings to determine which Snapchat users can view their "stories," block or remove friends, change when Chats are deleted, edit how their name appears, clear conversations, make audio or video calls, to highlight just a few of Snapchat's features.

14. At all times relevant herein, PNC Financial Services Group (hereinafter "PNC Bank"), Capital One Financial Corporation (hereinafter "Capital One"), TD Bank N.A. (hereinafter "TD Bank"), Bank of America, Republic Bank, Wells Fargo & Company (hereinafter "Wells Fargo"), and Truist Financial Corporation (hereinafter "BB&T") are "financial institutions" as defined by Title 18, Section 20.

C. Overview of the Fraud Scheme

15. Investigators learned that MASSA primarily uses social media platforms, such as Instagram, to recruit individuals to participate in a fraud scheme. Investigators identified MASSA's Instagram account under the username "Kayg0ldi." The "Kayg0ldi" Instagram account has over 343,000 followers. Investigators also identified various vanity name variations of the "Kayg0ldi" account during the course of this investigation. These included "theonlykayg0ldi" and "Kay Kay," (collectively hereinafter "Kayg0ldi"). The investigation revealed that Instagram account user "Kayg0ldi" routinely posted and continues to post, as recent as December 9, 2019, various photos or

videos, referred to herein as advertisements, often targeting Instagram viewers with bank accounts. Some examples of the advertisements are attached hereto as "Exhibit 1."

16. These advertisements, posted to "Kayg0ldi's" story, were often accompanied with photos of stacks of cash, United States Postal Service (hereinafter "USPS") money orders, and screenshots of bank account balances or receipts from various financial institutions. Some advertisements were videos posted to "Kayg0ldi's" story, of stacks of cash being counted, debit cards being flashed with cash or USPS money orders in view, or ATM receipts with cash. This is not an exhaustive list of the advertisements posted routinely on "Kayg0ldi's" Instagram story. Individuals interviewed during the course of this investigation explained that after viewing "Kayg0ldi's" story, they responded via direct message¹, often to a specific advertisement. During the direct message communication, "Kayg0ldi" provided these individuals with a variety of explanations as to how their bank account would be used for a legitimate and legal purpose. In those direct message communications, "Kayg0ldi" encouraged individuals to empty their bank accounts before providing their debit card and PIN to MASSA, in an effort to falsely allay any fears of losing money. Account holder "Kayg0ldi" arranged for these individuals to meet at a public place, communicating through direct message or via a cell phone number provided by "Kayg0ldi." Individuals interviewed during the course of this investigation stated that they met a woman later identified as MASSA and, in some instances, HERRIN, identified as MASSA's boyfriend at the time or her sister LEIRE. At those meetings, the individuals provided MASSA with their debit card, personal identification number ("PIN"), and in some instances, their online banking login information as well as answers to any security questions.

17. Once in possession of the individuals' debit cards and PINs, MASSA and her co-conspirators used the individuals' bank accounts to deposit various fraudulent financial instruments,

¹ Commonly referred to as a "DM."

including stolen USPS money orders, counterfeit Western Union money orders, and various counterfeit checks usually drawn from legitimate business accounts. MASSA's co-conspirators deposited the fraudulent financial instruments at various bank branches, ATMs, or through mobile deposits. While the funds were in the account but before the individual banks discovered the fraudulent financial instruments, co-conspirators used the debit cards to withdraw the funds. In this investigation, "cracked" cards are defined as the debit cards that have been used to deposit counterfeit financial instruments in furtherance of the fraud, and are often used to purchase legitimate financial instruments such as USPS money orders, to launder the proceeds from the cashed counterfeit checks and obfuscate the true source of the funds.

18. Co-conspirators used bank and ATM withdrawals, and purchased USPS money orders to deplete individuals' accounts before the banks discovered the fraud. The window of time between the fraudulent deposits and withdrawals was approximately 2-4 days. Once the deposits were discovered to be fraudulent, the account holder's balance would quickly become negative. When the individuals learned that their accounts were in a negative balance, many tried to contact MASSA, but were ignored and, in many instances, blocked from contact. In most instances, the USPS money orders the co-conspirators purchased with these "cracked" debit cards, were later cashed at various post offices or check cashing locations, primarily in New Jersey and Pennsylvania, by MASSA, HERRIN, LOGAN, LEIRE or other co-conspirators and or their associates.

19. Records obtained on the "Kayg0ldi" Instagram account identified conversations with multiple individuals where MASSA attempted to recruit people into the scheme.² Additionally,

² An Instagram account holder maintains the ability to deactivate and delete information and data from the account. Information or data that is deleted by an account holder is removed from Instagram servers at or around the time it is deleted by the account holder. As a result, the search warrant return on Kayg0ldi's Instagram account only produced the records available at that time, with no ability to retrieve deleted data to include direct messages.

investigators were able to obtain an array of advertisements posted to “Kayg0ldi’s” account, similar to those described by the various victims interviewed.

20. Investigators obtained direct message conversations between MASSA and others where MASSA explained how to recruit others and be convincing.

21. Investigators identified various social media platforms used by other co-conspirators including LOGAN, MCCRAE, LEIRE, HAINES, JOHNSON, MCDANIELS, AND MARTIN, particularly Instagram. Co-conspirators, similar to MASSA, used social media to advertise and recruit individuals to provide their bank account information, often posting advertisements very similar to ones posted by MASSA.

22. LOGAN, operating under various usernames on Instagram, to include “nlb_100k,” “100k_nlb,” “nlb_93k,” topopp_100k” posted advertisements to his “story,” primarily using “100k_nlb.” A sampling of these advertisements are attached hereto as “Exhibit 2.”

23. MCCRAE, operating under Instagram username, “realycwoody” posted similar advertisements. A sampling of these advertisements are attached hereto as “Exhibit 3.”

24. LEIRE, operating under Instagram username, “Onlyg0ldenLe” and Snapchat under username, “Le” posted similar advertisements. A sampling of these advertisements are attached hereto as “Exhibit 4.”

25. JOHNSON, operating under Instagram username, “Savage_Santa” and Facebook under username “Santaa_bag” posted similar advertisements. A sampling of these advertisements are attached hereto as “Exhibit 5.”

26. HAINES, operating under Instagram username “_adh23_” posted similar advertisements. A sampling of these advertisements are attached hereto as “Exhibit 6.”

27. MARTIN, operating under Instagram username “1hunit_mill,” posted similar advertisements. A sampling of these advertisements are attached hereto as “Exhibit 7.”

28. MCDANIELS, operating under Instagram username “chasesir100k,” posted similar advertisements. A sampling of these advertisements are attached hereto as “Exhibit 8.”

D. The Investigation

29. On or about July 31, 2018, USPS Office of the Inspector General (hereinafter “OIG”) received a report of suspicious activity regarding fifty-three USPS money orders. The report indicated that fifty-three USPS money orders were never recorded as “sold” but a significant number were subsequently deposited/cashed into various bank accounts. All the USPS money orders were issued from the same serial block³ and assigned to the Post Office in Berlin, New Jersey (hereinafter the “Stolen Money Orders”). Of the fifty-three Stolen Money Orders stolen, thirty were discovered deposited in various bank institutions during May, 2018, each in the amount of \$990 or \$995. These Stolen Money Orders did not have a clerk number imprinted and the date, post office zip code, and dollar amount were a different font than legitimately issued USPS money orders.

30. Investigators with the USPS OIG and USPIS conducted an investigation into the stolen USPS money orders that were fraudulently imprinted and cashed. Through subpoenas, investigators identified the bank accounts the stolen USPS money orders were deposited into. Investigators identified and interviewed several account holders whose accounts were used to deposit the stolen USPS money orders.

a. May 4, 2018 Fraudulent Activity - Victim “J.K.”

³ Every USPS money order has a unique serial number which can be used to identify the originating post office as well as the specific USPS employee assigned that money order as accountable property. The aforementioned stolen USPS money orders originated from money order block 2460829600-699, assigned to the Berlin, New Jersey Post Office.

31. Investigators identified an account holder, identified herein as "J.K.," who had two Stolen Money Orders deposited into his/her PNC personal bank account.⁴ The two Stolen Money Orders were deposited into J.K.'s account on or about May 4, 2018. Each Stolen Money Order was issued in the amount of \$995. J.K. was named as the payee for both Stolen Money Orders.

32. In October, 2018, investigators interviewed J.K. at his/her residence in Barrington, New Jersey. During that interview, J.K. told investigators that on or before May 4, 2018, he/she responded to an Instagram advertisement placed by Instagram account holder "Kayg0ldi." Investigators confirmed MASSA was the registered user for the "Kayg0ldi" account from August 16, 2011 to June 10, 2019.⁵ MASSA, using "Kayg0ldi," communicated with J.K. through Direct Message. In those communications, J.K. told investigators that MASSA told him/her that he/she could earn approximately \$5,000 by allowing MASSA to use his/her bank account for a friend's clothing line as a "tax write off." MASSA told J.K. that he/she would need to give up their bank card for an unspecified, but short, period of time.

33. On or about May 4, 2018, J.K. and MASSA agreed to meet at a McDonald's in Blackwood, New Jersey. When J.K. arrived at the location, he/she encountered MASSA and HERRIN. MASSA told J.K. the same story about a friend's clothing line and "tax write off." MASSA told J.K. that he/she would earn approximately \$5,000. MASSA asked for J.K.'s debit card, PIN number, and online account log-in information for his/her PNC account; a PIN, or Personal Identification Number, is required to authenticate an individual's access to a specified bank account. MASSA told J.K. that she would return the debit card quickly.

⁴The two stolen USPS money orders contained serial numbers 2460829651 and 2460829684.

⁵ Records obtained from Instagram revealed that the account was still active as of June 10, 2019, registered with email kaylaa.ileana@yahoo.com, gold22kay@gmail.com, and kaylaileana@yahoo.com, and phone number 609-592-2813.

34. On or about May 4, 2018, an unidentified person deposited two stolen USPS money orders, one into J.K.'s PNC Reserve Checking Account, and one into J.K.'s Spend Checking Account, totaling \$1,990. On or about May 11, 2018, three debit card transactions were conducted using J.K.'s Spend Checking Account, two purchases at two Wal-Mart stores, one for \$500.88 and another for \$450.88. The third transaction occurred at the Clementon Post Office, where a legitimate USPS money order was purchased for \$450.00 using J.K.'s "cracked" card. That USPS money order was subsequently cashed with the listed payee as James Hines. Both previously deposited stolen USPS money orders returned as altered/fictitious on or about May 18, 2019. On or about June 12, 2018, PNC closed J.K.'s accounts and the remaining negative account balance was charged off as a loss by PNC. J.K. made multiple attempts to contact MASSA through "Kayg0ldi" but was blocked. Because J.K. was blocked, he/she could not retrieve their prior correspondence. According to Instagram policy, after blocking an account, (direct) messaging threads with the blocked account will remain in the inbox of the account initiating the block, but the messaging feature will be disabled. If the account that was blocked attempts to send any direct messages, the messages will not be received and will not be delivered in the event the account is unblocked in the future. Instagram's policy does not record what happens to the blocked account holders' access to the direct messages, however based on victim interviews, all direct messages between the victims and "Kayg0ldi" were removed once the victims were blocked.

35. During his/her interview, J.K. identified a photograph of MASSA from her New Jersey Driver's License photo with no personal identifiers. J.K. also identified MASSA in a photo displayed on the "Kayg0ldi" account. Investigators learned that between approximately March 2017 and October 2018, MASSA and HERRIN were in a romantic relationship.

36. In October 2018, investigators received bank surveillance footage of activity related to the Stolen Money Orders. Fifteen of the Stolen Money Orders were deposited into approximately seven

different PNC Bank accounts, including J.K.'s PNC bank account. Based on the footage, investigators determined that the Stolen Money Orders were deposited at four separate PNC Bank branches in Stratford, Sicklerville, Cherry Hill, and Clementon, New Jersey. The Stolen Money Orders deposited into J.K.'s accounts occurred at two different PNC Bank branches, in Clementon and Stratford, New Jersey. Investigators identified an individual matching HERRIN'S physical description on at least one of the images provided by PNC Bank.

b. August 28, 2018 Fraudulent Activity – Victim “C.F.”

37. In or about October, 2018, investigators identified another individual, identified herein as “A.R.,” who reported fraudulent activity on an account that he/she maintained with his/her minor child, identified as “C.F.”

38. C.F. told investigators that he/she began corresponding with MASSA through Instagram on MASSA's “Kayg0ldi” account in response to social media posts on Instagram. C.F. corresponded with MASSA using the Instagram Direct Message feature. In those communications, C.F. said that MASSA told him/her that she had her own “brand” and that she would put C.F. on her payroll. MASSA said that she would pay C.F. for the using his/her account. MASSA provided C.F. with a cellular phone number to text, 856-839-1074. A person who identified themselves as “Kayla” sent multiple texts to C.F. Investigators learned that the telephone number provided by MASSA to C.F. was associated with HERRIN. Based on their conversations, on or about August 12, 2018, C.F. went to the Lindenwold Port Authority Transit Corporation (“PATCO”) Station, where he/she met MASSA and HERRIN. There, MASSA asked for C.F.'s Capital One debit card and PIN number. C.F. believed that, based on their conversation, MASSA was the same person he/she had been texting with.

39. Between August 13 and 14, 2018, four Western Union Money Orders,⁶ each imprinted for \$995.00, were deposited into C.F.'s Capital One account, totaling approximately \$3,980. On or about August 14, 2018, MASSA contacted C.F. through text messaging on the cellular phone number 856-839-1074, to give C.F. more instructions. MASSA told C.F. that the longer she had the card, the more money they would make. She also told C.F. that she usually kept cards for a full 5 business days, earning about \$2,000.

40. On or about August 15, 2018, C.F. attempted to contact MASSA through the "Kayg0ldi" Instagram account, but was unable to do so because he/she was blocked. C.F. attempted to contact MASSA using the cellular phone number 856-839-1074, they had used before, but was blocked from that number. Because C.F. was blocked, he/she was unable to retrieve their prior correspondence.

41. On or about August 17, 2018, the four Western Union Money Orders previously deposited into C.F.'s account were returned as altered/fictitious. C.F.'s bank account was overdrawn approximately \$3,964.56. Based on information from A.R. and C.F., Capital One subsequently closed the account because of a negative account balance of \$3,526.53.

42. Investigators reviewed bank surveillance footage from the Capital One branch located at 135 South 17th Street, Philadelphia, Pennsylvania, for August 13 and August 14, 2018. Investigators identified FELICIANO depositing the altered/fictitious Western Union Money Orders into C.F.'s bank account. Investigators learned that FELICIANO was the boyfriend of LEIRE, MASSA's younger sister.

43. Investigators reviewed bank surveillance footage at the same branch from August 14 and August 15, 2018. On those dates, bank surveillance footage recorded HERRIN withdrawing \$1,000 on each day, for a total of \$2,000, from C.F.'s account.

⁶The Western Union Money Orders contained the following serial numbers: 17-740316791, 17-740316796, 17-716301204 and 17-716301202.

44. Investigators learned that on August 14, 2018, C.F.'s Capital One debit card was used at the Clementon Post Office, located at 22 Berlin Road in Clementon, New Jersey. C.F.'s card was used to purchase a USPS money order, bearing serial number 2518072952, in the amount of \$980.00. Investigators obtained surveillance footage of the transaction and identified HERRIN as the person using C.F.'s card.

45. Investigators learned that on August 15, 2018, C.F.'s Capital One debit card was used at the Westville Post Office, located at 329 Broadway, Westville, New Jersey. C.F.'s card was used to purchase a USPS money order, bearing serial number 25314782804, in the amount of \$980.00. Investigators could not obtain surveillance footage of the transaction.

46. Investigators learned that both USPS postal money orders purchased with C.F.'s Capital One Card (purchased at the Clementon Post Office and Westville Post Office) were cashed on August 15, 2018, at One Stop Shoppe Check Cashing, 333 Sicklerville Road, Sicklerville, New Jersey. The listed payee and payer on both money orders was HERRIN, who provided his address.

c. July 25, 2018 Fraudulent Activity – Victim “M.D.”

47. Investigators identified and interviewed another victim, identified herein as “M.D.” in April 2019. M.D. told investigators that in or about July 2018, he/she responded to an Instagram advertisement posted by MASSA. M.D. said that he/she responded to an advertisement that he/she saw on both Instagram, posted by “Kayg0ldi,” and Snapchat, posted by “Kay Kay.” M.D. knew MASSA and HERRIN from a previous meeting in January 2018. Then, M.D. responded to a similar ad posted by MASSA but explained that despite providing her bank account information, her account was not used. M.D. did not know why but only stated that it did not work.

48. In or about July 2018, M.D. communicated with MASSA through Snapchat. M.D. responded to an ad with stacks of cash, asking “how?” to which MASSA replied, “where you from?”

MASSA and M.D. exchanged messages where MASSA explained that she had a business partner with a payroll system and that for some reason, she would have her business partner add M.D.'s name to the company and write a payroll check. MASSA reassured M.D. that the arrangement was legitimate and that it would take 3-5 business days to complete.

49. On or about July 25, 2018, M.D. agreed to meet MASSA at the TD Bank located at 1235 Blackwood Clementon Road, Clementon, New Jersey. There, he/she provided MASSA his/her TD debit card, PIN, and online banking information. M.D. stated that MASSA's boyfriend, HERRIN, was with MASSA at the TD Bank. M.D. stated that MASSA directed him/her to remove all funds from the account before providing the card to MASSA. That same day and into the following day (July 26, 2018), five altered/fictitious Western Union money orders, each imprinted for \$995.00, were deposited into three different accounts held by M.D. at TD Bank branches in New Jersey.

50. On or about Thursday July 26, 2018, M.D. met MASSA at a TD Bank located at 601 College Drive in Blackwood, New Jersey. There, at the direction of MASSA, M.D. removed \$700 from his/her TD account. The next day, M.D. met MASSA again at the same TD Bank, in Blackwood, New Jersey. There, MASSA directed M.D. to withdraw \$2,900 from his/her account and give it to MASSA, which M.D. did. According to M.D., almost immediately, MASSA directed him/her to return again to the same TD Bank and withdraw whatever funds remained in the account. M.D. was unable to make the withdrawal because TD Bank suspected fraudulent activity on his/her account. M.D. contacted MASSA, who was still waiting in the parking lot, through Instagram and notified MASSA about the fraud. MASSA and HERRIN drove off with the money and M.D.'s debit card. M.D. stated he/she never received payment from MASSA or HERRIN and never received his/her debit card. M.D. told

investigators that he/she attempted to contact MASSA but was unsuccessful because MASSA blocked his/her on Instagram. TD Bank subsequently closed M.D.'s accounts with a \$3,738 loss.⁷

51. Investigators reviewed TD Bank surveillance footage from July 25, 2018, and identified an individual matching HERRIN's description depositing two of the five altered/fictitious Western Union money orders into M.D.'s TD bank accounts at a TD Bank in Stratford, New Jersey. On July 26, 2018, an individual matching HERRIN's description, wearing the same clothes seen on bank surveillance footage the day before, deposited two more altered/fictitious Western Union money orders into M.D.'s TD bank account at the TD Bank in Stratford, New Jersey. Later on that same day, an individual matching HERRIN's description, wearing the same clothes seen earlier in the day and the day prior, was recorded on bank surveillance footage at the drive-through TD Bank ATM in Gloucester Township, New Jersey, driving a black Nissan Maxima with tinted windows, and depositing the fifth altered/fictitious Western Union money order into M.D.'s TD bank account. Investigators subsequently learned that at the time of this incident, MASSA owned a black Nissan Maxima, bearing New Jersey registration LE-CD59 (hereinafter the "Black Nissan"). As described throughout this Affidavit, the Black Nissan was observed, and in many instances recorded, during transactions linked to similar fraudulent activity during this investigation.

52. Investigators reviewed records obtained from Western Union regarding the Western Union money orders deposited into M.D. and C.F.'s accounts.⁸ Western Union representatives identified "David's Check Cashing," located in New York, as the issuing agent for the money orders, and advised there were a total of five hundred ninety-nine (599) Western Union money orders within those serial

⁷ M.D. had to enter a repayment plan to settle his/her debt to TD Bank.

⁸ The serial numbers of those deposited money orders were identified as: 17-740316789, 17-740316791, 17-740316796, 17-716301202, 17-716301204, 17-716301546, 17-716301542, which fell within two Western Union money order blocks flagged by Western Union as counterfeit.

number blocks flagged as counterfeit. Western Union representatives advised the potential loss exposure was approximately \$596,005, calculated based on the value of each money order at \$995.00. Three hundred thirty-one (331) of the five hundred ninety-nine (599) aforementioned Western Union money orders were presented for payment at various financial institutions including Bank of America, TD Bank, Navy Federal Credit Union, Capital One and PNC Bank. Navy Federal Credit Union advised they actually lost approximately \$20,383.85, and were exposed to approximately \$36,500 in loss.

d. January 31, 2019 Fraudulent Activity - Victim A.S.

53. On February 5, 2019, Winslow Township Police officers conducted a motor vehicle stop at 250 Sicklerville Road in Sicklerville, New Jersey, on the Black Nissan, but driven by LOGAN. There were two additional occupants inside the vehicle, FELICIANO and MCDANIELS. Police dispatch identified outstanding warrants for FELICIANO and LOGAN, resulting in their arrests on scene. Winslow Police officers conducted a probable cause search and located thirty-nine checks issued to "Nissan Turnersville," by Bank of America, shoved inside the vehicle's sunroof, and two Bank of America debit cards in the names of people who did not match any of the vehicle's occupants. Winslow Police officers also discovered multiple Bank of America withdrawal slips located in the center console of the vehicle, and two blank USPS money orders, each purchased for \$850.00, located in the front seat. All thirty-nine "Nissan Turnersville" checks were issued to Keith Williams in the amount of \$88.00 each. LOGAN and FELICIANO told the Winslow Police officers that they did not know who the debit cards or checks belonged to. From LOGAN, Winslow Police officers recovered \$2,690.65 in cash, and from FELICIANO, Winslow Police officers recovered \$2,584.00 in cash. During the course of the vehicle search, LEIRE arrived on scene and was captured on body camera footage.

54. After recovering the Nissan Turnersville checks, investigators contacted Nissan Turnersville in reference to the Nissan Turnersville checks found with LOGAN, FELICIANO, and

MCDANIELS. Nissan Turnersville provided investigators with a list of all the fraudulent checks issued from Nissan Turnersville's Bank of America account during the month of February 2019, as well as a sampling of the check images. From that list, investigators identified the listed payees and banks where the unauthorized checks were deposited. In total, between January and August 2019, there were approximately six hundred ninety-seven checks fraudulently issued using Nissan Turnersville's account information, and deposited into approximately forty-five different bank accounts, totaling approximately \$128,380.03. Each of the six hundred ninety-seven checks were returned from the banks where they were deposited because the checks were deemed fraudulent.

55. Based on information provided by Nissan Turnersville, investigators located and interviewed several individuals who had Nissan Turnersville checks deposited into their accounts. On June 10, 2019, investigators interviewed an individual identified herein as "A.S.," who had approximately fifty Nissan Turnersville checks deposited into his/her Bank of America account that he/she shared with his/her mother, A.T. Each of the fifty check were issued for \$88.00, totaling approximately \$4,400.00. The checks were deposited between January 31, 2019 and February 1, 2019, and all were returned as fraudulent. A.T. had previously filed a report with Washington Township Police Department regarding the fraudulent activity on the joint bank account. A.S., sixteen at the time, provided a written statement to Washington Township Police officers on February 1, 2019 and later to investigators. According to A.S., MASSA posted an advertisement on Snapchat about making money, to which A.S. responded. A.S. provided investigators with screenshots of the conversation on Snapchat. In that conversation, MASSA told A.S. that small checks would be deposited into A.S.' account from a legitimate payroll company. MASSA asked for the passcode, and later asked A.S. to contact the bank to raise the maximum ATM withdrawal limit.

56. The conversation continued between A.S. and MASSA via text. A.S. provided screenshots of the communication to investigators where MASSA issued instructions and asked A.S. to raise his/her cash withdrawal limit, a copy of which are attached hereto as "Exhibit 9." The phone number communicating with A.S. was listed as 609-592-2813. Subscriber records obtained by investigators shows that this telephone number was subscribed to KAYLA MASSA, at 515 Mullica Hill Road, Glassboro, New Jersey, with an effective date of June 09, 2018. Investigators obtained records confirming that this communication between A.S. and MASSA occurred on or about February 1, 2019. During the interview with A.S., he/she stated MASSA arrived at his/her home in Blackwood, New Jersey, to pick up his/her debit card in the Black Nissan. A.S. told investigators that MASSA was in the back seat of the Black Nissan and MASSA's sister LEIRE, identified by A.S., was seated in the front passenger seat with a male driver, who A.S. could not identify. At one point, MASSA messaged A.S. with the following request:

MASSA: You have cash app? Like linked on your account Did you get any text from the bank yet Can I do it again for tm? I need a favor Send \$1500 to this #8563530473

57. A.S. provided a copy of an email received by Bank of America, which stated in the subject line, "You've added Alex to your list of Zelle⁹ recipients." Based on the image, the email was sent on or about February 1, 2019. The body of the email noted the addition of "Alex" along with telephone number 856-353-0473, with a "send money" link below the name and phone number. During the text exchange with A.S., MASSA directed A.S. to send \$1,500.00 through Cash App¹⁰ to 856-353-

⁹ "Zelle" is a digital platform utilized to send money directly between most U.S. bank accounts, typically within minutes. With an email address or mobile phone number, individuals can send and receive money, regardless of where they bank.

¹⁰ "Cash App," owned by and operated by Square Inc., is a digital platform utilized to send money, spend money, save money, and buy Bitcoin. Cash App supports debit and credit cards from Visa, Mastercard, American Express, and Discover. ATM, PayPal, prepaid bank cards, and business debit cards are not supported as of 12/2019. Cash App offers a Cash Card, which is a free, customizable debit card connected to an individual's Cash App balance and can be used anywhere Visa is accepted.

0473. Subscriber records obtained by investigators shows that this telephone number was subscribed to ALEX HAINES at 417 Glover Street, Woodbury, New Jersey, with an effective date of July 15, 2018. Investigators reviewed documents from Bank of America showing that on or about February 1, 2019, two attempts to transfer funds to Square username "Never Chilling" occurred, but both were declined, citing "fraud protection" as the reason. Investigators confirmed that the Cash App account "Never Chilling" was registered to HAINES, who provided his date of birth of 10/12/1992, phone number 856-353-0473, email address of "adhaines92@gmail.com," with a Cash App username "neverchilling," and a listed address of 417 Glover Street, Woodbury, New Jersey.¹¹

58. Investigators were unable to retrieve bank surveillance footage from A.S.'s account. However, the Bank of America ATM used to withdraw funds from A.S.'s account, located at 407 Egg Harbor Road, inside the Washington Center Shops Plaza in Sewell, New Jersey, has been frequently used by the organization, particularly, FELICIANO and LOGAN. Washington Township Police officers conducted a motor vehicle stop with FELICIANO, LOGAN, and MASSA, at the same Bank of America ATM at approximately 4:00 a.m. in March 2019.

59. The first deposits of fraudulent Nissan Turnersville checks into A.S.' Bank of America account were made at the Bank of America ATM, located in Woodbury, New Jersey on January 31, 2019. The Bank of America ATM in Woodbury, New Jersey, was frequently used by FELICIANO and LOGAN during the course of this investigation.

60. On February 1, 2019, A.S.'s debit card was used to purchase one USPS money order at the Pitman Post Office located at 55 N Broadway Pitman, New Jersey. The USPS money order was redeemed on or about February 25, 2019 by Raquon Clarke, at the Marrs Group LLC, doing business as

¹¹ HAINES' virtual Cash App card was issued March 06, 2017.

United Check Cashing, located in Williamstown, New Jersey. Raquon Clarke is a known associate of LOGAN.¹²

e. February 01, 2019 Fraudulent Activity – Victim “B.N.”

61. In April 2019, investigators interviewed an individual identified herein as “B.N.” regarding approximately twenty-five Nissan Turnersville checks, each issued for \$88.00, deposited into B.N.’s Bank of America account on or about February 1, 2019 in the amount of \$2,200, all of which were later determined to be altered/fictitious. Investigators spoke to B.N., who initially claimed to have no knowledge of any fraudulent activity, but later provided a detailed account of his/her interaction with MCDANIELS that led to the fraudulent activity. B.N. admitted to providing his/her Bank of America card to MCDANIELS, who paid him/her \$150 in cash in exchange for the debit card. B.N. told investigators that MCDANIELS never returned the debit card. B.N. told investigators that he/she contacted MCDANIELS after seeing the advertisement on MCDANIELS’ Facebook account. MCDANIELS asked B.N. if he/she had any other bank accounts or any friends with bank accounts that would be interested in making money. B.N. said that he/she did not provide MCDANIELS with any other accounts.

62. Investigators reviewed Bank of America surveillance footage from B.N.’s account activity. From this footage, investigators identified a light-skinned black male wearing a dark colored hooded sweatshirt with the hood partially obstructing the upper half of his face. The individual in the footage matched MCDANIELS’ physical description and attire previously identified by investigators during a review of social media and other bank surveillance footage. Investigators learned that on

¹² On February 20, 2017, Glassboro Police Department officers responded to a suspicious vehicle incident involving LOGAN, Raquon Clarke, Rowhan Thomas, and Jordan Murray. During the course of this investigation, investigators identified USPS money orders purchased with “cracked” cards redeemed by Jordan Murray and Rowhan Thomas.

February 1, 2019, MCDANIELS deposited twenty-five Nissan Turnersville checks, for approximately \$2,200, into B.N.'s account at the Bank of America drive-through ATM located in Voorhees, New Jersey. MCDANIELS walked up to the ATM on foot, despite it being a drive-through ATM, which is consistent with previous instances captured on bank surveillance footage of MCDANIELS and other co-conspirators. At the time of the deposit, MCDANIELS was with another individual, who could be seen wearing a "BAPE" brand shark hooded sweatshirt, which retails for approximately \$475.00. The BAPE sweatshirt was dark in color, camouflage, with a distinctive hood that replicated a shark head with shark eyes and teeth outlined on the hood. On February 2, 2019, at 4:00 a.m., an individual attempted to withdraw funds from B.N.'s account. That person, wearing a nearly identical BAPE shark hooded sweatshirt and similar in height, weight, and build to the person seen with MCDANIELS the prior day, concealed his/her face from camera view. That transaction was declined.

63. Later that same morning, an individual wearing fitting MCDANIELS' description and wearing the same dark colored hooded sweatshirt, successfully withdrew \$1,500 from B.N.'s account using a drive-through ATM in Williamstown, New Jersey.

64. On the same day, February 2, 2019, B.N.'s card was used to purchase one USPS money order for \$695.00 at the Williamstown Post Office, located in Williamstown, New Jersey. On February 8, 2019, that same USPS money order was deposited into a Wells Fargo bank account without any information filled out, including a payee. Investigators identified the bank account into which the USPS money was deposited belonged to Semya McDaniels, a known associate of MCDANIELS. On March 22, 2019, B.N.'s account was closed with a negative account balance of approximately \$2,496.44.

f. February 13, 2019 Fraudulent Activity – Victim "T.F."

65. In February 2019, investigators learned of another individual, identified herein as "T.F." whose accounts were used in the fraudulent activity. Between February 13, 2019 and February 15,

2019, eight Nissan Turnersville checks, totaling \$4,490.14, were deposited into T.F.'s TD Bank account. Each of these check was subsequently deemed fraudulent. Investigators learned that T.F.'s debit card was used to purchase three USPS money orders, totaling \$2,490.00.¹³ Two of these USPS money orders, purchased with T.F.'s "cracked" card, were deposited into LEIRE's Wells Fargo bank account¹⁴ and featured in two different advertisements posted on social media by LEIRE. The first advertisement was posted on "g0ldenle's" Instagram story and the second on "Le's" Snapchat story (the Snapchat advertisement image is attached hereto as "Exhibit 10"). Investigators confirmed that both social media accounts were associated with LEIRE. Investigators reviewed T.F.'s bank statements during the timeframe of the fraudulent activity and identified several purchases and withdrawals.

66. Between February 14 and February 16, 2019, funds were withdrawn from T.F.'s bank account through an ATM, in three separate transactions, in \$760.00 increments, totaling \$2,280.00, at three different TD Bank ATMs in South Jersey, including Collingswood, Oaklyn, and Haddon Heights. As discussed earlier, on February 15, 2019, T.F.'s debit card was used to purchase one USPS money order, in the amount of \$850.00, at the Collingswood Post Office. This USPS money order was deposited into LEIRE's Wells Fargo account on or about February 21, 2019.

67. On February 16, 2019, T.F.'s card was also used to purchase two USPS money orders, each issued for \$820.00, at the Oaklyn Post Office. One of these USPS money orders was deposited into LEIRE's Wells Fargo account, also on or about February 21, 2019.

68. As of April 5, 2019, T.F.'s TD Bank student checking account had a negative balance of \$2,550.99. As of March 31, 2019, T.F.'s TD Bank savings account had a negative balance of \$2,455.00.

¹³ Total does not include tax or money order fees.

¹⁴ Both USPS money orders were deposited blank, with no identifying information completed, including the payee or payer.

69. In March, 2019, investigators identified an advertisement posted on goldenle's Instagram story, where two USPS money orders were displayed as well as a stack of U.S. currency fanned out, with the words "SC me if interested. Let's get to that bag YKTV come fw me!" (SC = Snapchat, YKTV = You know the vibes). Investigators identified the sale of the USPS money orders displayed in LEIRE's advertisement and confirmed both USPS money orders were purchased using a "cracked" card belonging to a different victim, identified as A.V. These USPS money ordered were purchased on March 5, 2019 at the Clayton Post Office, located in Clayton, New Jersey. Investigators learned that A.V. maintained a Bank of America account. Investigators also learned that on March 4, 2019, A.V.'s account had approximately \$2,436.00 of deposits of fraudulent checks. Before Bank of America recalled the funds for fraud, two USPS money orders were purchased, each for \$980.00. The first USPS money order was redeemed by LEIRE on or about March 11, 2019, at Finanza Servizi LLC, doing business as United Check Cashing, located in Clementon, New Jersey. The second money order was redeemed by FELICIANO on or about April 22, 2019, at Paramount Financial, doing business as Cash Out Check Cashing, located in Deptford, New Jersey.

70. During the course of their investigation, investigators identified a third USPS money order deposited into LEIRE's Wells Fargo account on or about December 4, 2018. The third USPS money order, issued for \$700.00, had the payee listed as "Leire Massa" with an address listed as "615 Clay St Riverside, NJ 08075¹⁵" and the payer listed as "Khris Fleeteam¹⁶" with an illegible address listed in Asbury Park, New Jersey. Investigators confirmed that the third USPS money order was purchased on December 4, 2018, at the Clementon Post Office, located in Clementon, New Jersey, using another "cracked" debit card (belonging to a person referred to herein as "A.T.-1"). Investigators

¹⁵ Investigators confirmed this address is associated with LEIRE and the MASSA family.

¹⁶ Khris Fleeteam has been identified by investigators as FELICIANO's alias/name on Facebook.

reviewed A.T.-1's bank statements and confirmed that two altered/fictitious Western Union money orders were mobile deposited into A.T.-1's account on December 3, 2018. This was one day before the USPS money orders were purchased. Both the Western Union money orders were subsequently deemed fraudulent. Before the Western Union money orders were deemed fraudulent, multiple ATM withdrawals and debits were made on A.T.-1's account, including the purchase of the \$700.00 USPS money order that was subsequently deposited into LEIRE's account on the same day. A.T.-1's account was overdrawn, resulting in a loss to Republic Bank of approximately \$1,201.65.

g. March 21, 2019 Fraudulent Activity – JOHNSON & TD Bank

71. Investigators worked cooperatively with Nissan Turnersville during the course of this investigation. As Nissan Turnersville identified fraud on their business account, they provided the fraudulent checks to investigators for follow up. Investigators utilized this information to identify additional bank accounts compromised in the fraud scheme. Investigators provided this information to the corresponding banks where the fraudulent checks were deposited. Bank of America utilized this information to run internal data analytics and identified associated fraudulent accounts to include individual "O.N's" account. On or about March 21, 2019, approximately \$12,514.65 in fraudulent checks were deposited into O.N.'s account at the Southwood Bank of America ATM, located in Woodbury, New Jersey. These deposits were conducted by FELICIANO, wearing a dark colored puffy Polo jacket with the hood partially obscuring his face. JOHNSON was observed behind FELICIANO while the deposits were conducted. During these deposits, JOHNSON was observed holding what appeared to be ATM deposit slips. Subsequent to the deposits, JOHNSON, FELICIANO, and another unidentified male were observed on bank surveillance footage congregating in front of the ATM. On or about March 25, 2019, all \$12,514.65 returned for fraud, and the account was force closed on approximately May 7, 2019.

72. Subsequent to these deposits, investigators identified JOHNSON's social media accounts, to include Instagram and Facebook, under the following names, "Savage_Santa" and "Santaa_baggy." JOHNSON utilized both accounts to recruit individuals in furtherance of the fraud scheme, utilizing the same recruitment manner as MASSA, LEIRE, LOGAN and others involved in the conspiracy. Investigators utilized information posted on JOHNSON's accounts to locate additional fraudulent activity, which was subsequently provided to the respective banks for follow up. From this, for example, TD Bank utilized internal data analytics to locate approximately 35 accounts with confirmed fraudulent activity. TD's risk exposure from these accounts totaled approximately \$165,030.23 with an actual loss of approximately \$15,299.18. Investigators observed JOHNSON on TD Bank's surveillance footage tied to 19 of the accounts with fraudulent activity. A sampling of fraudulent activity provided by TD Bank involving JOHNSON is outlined below:

73. **May 29, 2019 Fraudulent TD Bank Activity** – Investigators observed JOHNSON on TD Bank surveillance footage on May 29, 2019, at a TD Bank ATM located in Westampton, New Jersey. JOHNSON was observed during a six minute time frame conducting fraudulent deposits into at least four different TD Bank accounts, utilizing the same listed payer and account number on all of the fraudulent checks. At approximately 7:33 PM, JOHNSON was observed on TD Bank ATM surveillance footage depositing one fraudulent check into "S.A.'s" account for \$4,576.90, drawn off a Capital One account with Heavy & General Laborers as the listed payer. At approximately 7:35 PM, JOHNSON was observed in the background¹⁷ as one fraudulent check was deposited into "M.P.'s" account¹⁸ for \$4,768.86, drawn off the same Capital One account with Heavy & General Laborers as the

¹⁷ Investigators identified the individual in the photos as a close associate of JOHNSON and also involved in the fraud scheme.

¹⁸ M.P. opened his/her account the same day the fraudulent deposits occurred. M.P. also lived in the same apartment complex as S.A. based on TD records.

listed payer. At approximately 7:37 PM, JOHNSON deposited one fraudulent check into “K.B.’s” account for \$4,378.45, again drawn off the same Capital One account with Heavy & General Laborers as the listed payer. At approximately 7:39 PM, JOHNSON deposited one fraudulent check into “P.T.’s” account for \$4,275.65, again drawn off the same Capital One account Heavy & General Laborers as the listed payer. No funds were withdrawn from S.A., K.B., or P.T.’s accounts before the checks returned for fraud on June 3, 2019. M.P.’s account, however, had another fraudulent check, issued for \$4,922.17, mobile deposited into his/her account on May 31, 2019, drawn off a Fulton Bank account with the Township of Mantua Joint Municipal Court Bail account as the listed payer.¹⁹ However, no funds were removed before TD closed M.P.’s account on or about June 25, 2019.

74. **TD Bank Account Holder “D.R.”** – On approximately September 9, 2019, investigators observed JOHNSON on TD Bank surveillance footage at a TD Bank ATM located in Bayonne, New Jersey. JOHNSON deposited one fraudulent check into “D.R.’s” account for \$4,945.00, drawn off a routing number associated with the Federal Reserve Bank,²⁰ and Moneygram Payment System as the listed payer. On or about September 10, 2019, a \$500.00 withdrawal was conducted at a TD ATM, located in Gloucester, New Jersey.²¹ On or about September 16, 2019, D.R.’s debit card was utilized at Avis Rent A Car, located in Philadelphia, Pennsylvania, for approximately \$1,059.72.²² On or about September 27, 2019, D.R.’s account was debited \$29.75 by Avis Rent A Car, for payment of tolls. On or

¹⁹ Republic Bank recalled the funds from this deposit as the check was issued fraudulently off the Township of Mantua’s Joint Municipal Court Bail account.

²⁰ The fraudulent check had “1st Members 1st Federal Credit Union” listed as issuing bank, despite the routing number belonging to the Federal Reserve Bank. Throughout this investigation, investigators identified similar instances of this, where routing numbers on the fraudulent checks did not correspond to the issuing bank displayed on the checks.

²¹ No surveillance footage was provided for this withdrawal.

²² Throughout the course of this investigation, investigators identified multiple rental vehicles utilized during the course of the fraud scheme.

about November 13, 2019, TD Bank closed D.R.'s account and sent the remaining negative balance to collections.

75. **TD Bank Account Holder "N.B-M"** – On approximately September 11, 2019, JOHNSON was observed on TD Bank surveillance footage at the same TD Bank ATM located in Bayonne, New Jersey, depositing one fraudulent check into "N.B-M.'s" account for \$4,900.00, purported to be drawn off a Chase²³ account with PPT Management as the listed payer. Before the funds returned as fraudulent, multiple transactions were conducted to include a \$743.00 withdrawal on approximately September 12, 2019, at a non TD Bank ATM located in Camden, New Jersey. Three CashApp transfers were sent on the same date to CashApp Username "ST8 Paper," totaling approximately \$1,350.00. The initial check returned for fraud on September 13, 2019. TD Bank suffered a loss of approximately \$2,348.34, as a result of fraudulent activity on N.B-M.'s account.

h. March 22, 2019 Fraudulent Activity - Victim "M.H."

76. On March 22, 2019, Glassboro Police Department officers received a report of fraud from a juvenile victim who suffered a loss of \$700. Investigators spoke to the juvenile victim, identified herein as M.H., and learned that M.H. responded to an advertisement posted by MASSA. M.H. and MASSA exchanged messages through Instagram direct messenger approximately three days earlier. In those messages, MASSA made her pitch to obtain M.H.'s debit card. An excerpt of the conversation is attached hereto as "Exhibit 11." Later, MASSA met M.H. in person, took M.H.'s debit card and online banking information. After, MASSA stopped communicating with M.H. and never returned the debit card.

77. M.H. provided investigators with the telephone number provided by MASSA, 609-592-2813. Subscriber records obtained by investigators shows that this telephone number was subscribed to

²³ The routing number listed on the check corresponded to a Federal Home Loan Bank.

KAYLA MASSA, at 515 Mullica Hill Road, Glassboro, New Jersey, with an effective date of June 09, 2018. MASSA's phone records show a call placed by MASSA to M.H.'s phone on March 19, 2019.

78. Investigators learned that the fraudulent checks were drawn from two different business accounts, "Bakkaleh Arabeyeh Inc." and "Marksmen Brokerage House," both out of Palm Harbor, Florida. The checks drawn from "Bakkaleh Arabeyeh Inc." were deposited into M.H.'s account on March 20, 2019, for \$380.00 and \$320.00, and the checks drawn from "Marksmen Brokerage House" were deposited on March 21, 2019, for \$400.00 and \$470.00.

79. Investigators obtained surveillance footage from TD Bank related to activity on M.H.'s account. Investigators reviewed footage of an ATM inside Rowan University Student Center, in Glassboro, New Jersey, recorded on March 20, 2019. The footage, from 7:52 a.m., showed a light-skinned black male wearing a red puffy jacket, attempting to conceal the lower half of his face. The individual in the footage matched LOGAN's physical description and attire previously identified by investigators during a review of social media and other bank surveillance footage. Additional surveillance footage was obtained from Rowan University showing the male, believed to be LOGAN, entering the passenger side of the Black Nissan parked in front of the Student Center. Data from License Plate Reader (LPR) cameras in the area confirmed that the vehicle was the Black Nissan.

80. On June 28, 2019, at approximately 1:06 p.m., Glassboro Police Department officers conducted a motor vehicle stop on a gold Ford Taurus bearing New Jersey license plate D61-LJK, registered to MASSA. The vehicle was operated by LOGAN and had two additional passengers, FELICIANO and MARTIN. Police officers conducted a probable cause search of the vehicle and discovered various items inside the vehicle including multiple debit cards issued to people not in the vehicle as well as postal money orders not yet issued to a specific person. The search was concluded

and the vehicle, along with cell phones belonging to LOGAN, FELICIANO, and MARTIN were detained pending search warrants.

81. Upon execution of multiple search and communication data warrants from the June 28, 2019 motor vehicle stop, investigators reviewed data extracted from the cell phones belonging to LOGAN, FELICIANO, and MARTIN. Content from two of the cell phones, one retrieved from LOGAN's person and another retrieved from the pocket of a jacket located on the driver's seat of the vehicle, revealed conversations between LOGAN and other co-conspirators including MASSA, HAINES, and FELICIANO. During these conversations, seemingly unrelated individuals' names, their financial institutions, and account access information, including their online login details such as usernames and passwords and last four of social security numbers, were exchanged. Additionally, during these conversations, photographs of legitimate business checks were also exchanged. During the course of this investigation, investigators found account and routing information from these (and other) legitimately issued checks were used to manufacture fraudulent checks. These counterfeit checks were usually deposited into bank accounts of individuals "recruited" through social media.

82. On or about March 18, 2019, LOGAN engaged in a text conversation with an unknown person utilizing phone number 585-309-1211. The unknown person texted LOGAN a photograph of check number 2877, issued by "Bakkaleh Arabeyeh Inc.," to Atlantic Trucking Group for \$660.00, with the number "19-0766" listed in the subject line. This check image had the same account and routing information as the fraudulent checks deposited into M.H.'s account on March 20, 2019. Additionally, on or about March 20, 2019, LOGAN took a cell-phone photograph of a computer screen capturing an unidentified person's online Bank of America account ending in 8724, sending \$2,400.00 via an online money transfer to M.H.'s account.

83. On or about March 20, 2019, a brief text message conversation occurred between LOGAN and a contact listed as "Baby," with a phone number of 609-592-2813. Subscriber records obtained by investigators show that this telephone number was subscribed to KAYLA MASSA, at 515 Mullica Hill Road, Glassboro, New Jersey, with an effective date of June 09, 2018. An excerpt of the conversation is as follows:

MASSA M*****H****01 for the username and password

LOGAN does not immediately reply, however MASSA continues to text LOGAN the following:

MASSA 1** C***** Ct Blackwood, NJ 08012 United States

The username, password and address have been redacted, but the information was identified by M.H. as his/her account.

i. July 2019 Fraudulent Activity - Victim Woodbury Nissan

84. In September 2019, investigators interviewed T.W., an executive at Woodbury Nissan, regarding fraudulent activity associated with Woodbury Nissan. T.W. told investigators that eleven checks, totaling approximately \$13,828.10 were fraudulently issued from Woodbury Nissan's operating business account during July 2019. Investigators identified legitimate checks issued to Woodbury Nissan by various car dealerships and automotive businesses from data located on LOGAN's cell phones that were seized and searched by Glassboro Police Department in June, 2019.²⁴ Investigators also recovered conversations and images exchanged between LOGAN and another co-conspirator, HAINES²⁵ that detailed components of the fraud scheme. A majority of the images found on LOGAN's cellular telephone that contained information about car dealerships and automotive businesses came

²⁴ Investigators reviewed data extracted from various cell phones, to include two cell phones, retrieved on or around LOGAN's person from the June 28, 2019 vehicle stop involving LOGAN, MARTIN, and FELICIANO.

²⁵ Victim A.S. was directed to send money electronically to HAINES using phone number 856-353-0473, as outlined in paragraph 51.

from phone number, 267-772-8043. At least one image sent from phone number 856-353-0473 depicted two overlapping FedEx envelopes, the first one clearly addressed to Dealer Trades, Woodbury Nissan, HAINES' employer.

85. Subscriber records obtained by investigators show that 856-353-0473 was subscribed to ALEX HAINES, at 417 Glover Street, Woodbury, New Jersey, with an effective date of July 15, 2018. Subscriber records obtained by investigators show that 267-772-8043 was not subscribed to any listed person. Based on the images that were exchanged between the 267-772-8043 number and LOGAN, I believe this telephone was used by HAINES to transmit images and information to LOGAN.

86. Investigators learned that at the time of these contacts, HAINES was employed by Woodbury Nissan. T.W. told investigators that HAINES started with Woodbury Nissan in September 2015 as a lot attendant. As a lot attendant, HAINES was responsible for preparing vehicles for dealer trades as well as picking up vehicles as a result of dealer trades.²⁶ This entailed picking up and dropping off payment checks for the dealer trades when applicable. T.W. explained that an employee identified herein as H.G. was the Inventory Manager and handled all dealer trades. T.W. also explained that during his time as a Lot Attendant, HAINES was H.G.'s assistant and would work directly with him/her. T.W. said that HAINES had direct access to H.G.'s office located on the showroom floor, which was usually locked with an electronic door code because of the sensitive documents, such as dealer jackets and financial documents, located inside. T.W. stated that the door code does not routinely change and could not recall the last time it was changed. T.W. stated that the code likely was unchanged from when

²⁶Dealer trades are typically conducted when a particular vehicle a customer is interested in purchasing is not in stock at the customer's current dealership but is in stock at another dealership nearby. In order to facilitate the sale, the dealership would identify the other dealerships in the region where the particular vehicle requested is in stock and initiate a dealer trade, often trading inventory. Sometimes the dealership requires the vehicle to be purchased outright without initiating a dealer trade, at which time a check would be issued from one dealership to another. Sometimes the cost of the vehicles are not commensurate at which time one dealership would issue a check to offset the price difference.

HAINES worked as a Lot Attendant, and that HAINES was provided the code during his time as H.G.'s assistant. T.W. stated it was not unusual for HAINES to be in H.G.'s office. Based on HAINES' experience as a Lot Attendant and his work with dealer trades, I believe he had intimate knowledge of the process and the amount of money involved with dealer trades.

87. T.W. stated that HAINES was promoted to Parts Receiver in April 2019. As a Parts Receiver, HAINES received mail and packages, including checks, addressed to Woodbury Nissan. According to T.W., employees were directed not to open any mail, and instead to deliver unopened mail to the relevant party. T.W. told investigators that when HAINES received a payment for a dealer trade via FedEx/UPS/Postal, he delivered it to H.G., the inventory manager. H.G. coded the check in their internal system, then returned it to HAINES for delivery to the Accounting Department.

88. T.W. said that each dealership had a unique code which H.G. notated on the checks upon receipt. Investigators provided T.W. with approximately twenty-four check images retrieved from LOGAN's cell phones, all of which were issued to Woodbury Nissan legitimately. The twenty-four checks were issued from sixteen car dealerships and automotive shops throughout New Jersey and some cities in Pennsylvania. From those business check images, investigators confirmed fraudulent activity on at least twelve accounts. T.W. stated that based on the photos of the twenty-four checks, many already had the unique code written on the check, indicating they were already processed by H.G. Additionally, T.W. advised the background of various images reviewed matched that of the hallway, staircase or office located inside Woodbury Nissan. Investigators provided T.W. with two Nissan Woodbury check images retrieved from a conversation between LOGAN and phone number 267-772-8043, both of which had the same black sneaker with a large white Nike swoosh on the top of the sneaker belonging to the person taking the photo. Investigators reviewed live video footage

investigators reviewed live video footage from Nissan Woodbury's surveillance system in September 2019 matching the shoes worn by HAINES on the day.

j. June 13, 2019 Fraudulent Activity - Victim Joel's Auto Technology and M.T.

89. During a review of LOGAN's phone, investigators identified an image of a Joel's Auto Technology check, check number 8410, dated June 21, 2019, in the amount of \$123.86, made payable to Woodbury Nissan, and with an accompanying Nissan Woodbury invoice number 654141, that was sent to LOGAN's phone from 267-772-8043. Investigators confirmed with the owner of Joel's Auto Technology that there had been fraudulent activity on his business account during June, 2019. Investigators reviewed Joel's Auto Technology's banking records and identified eight fraudulent checks drawn from Joel's Auto Technology's bank account. These checks were deposited or attempted to be deposited into six different accounts, for a total of approximately \$15,082.12. One of these fraudulent checks, issued for \$2,862.18, was deposited into a BB&T account held by individual hereinafter referred to as M.T.

90. Investigators located various images on LOGAN's phone associated with an individual identified herein as "M.T." and his/her BB&T account. The first image was created on or about June 24, 2019 and depicted an individual in red pants sitting in a vehicle with check number 8463 purported to be issued by Joel's Auto Technology and made out to M.T. for \$2,862.18. A second image on LOGAN'S phone depicted a BB&T deposit receipt dated June 24, 2019, with a time stamp of 5:00 p.m., confirming a deposit of \$2,862.10²⁷ into a BB&T checking account ending in 8840. This check was deposited with a debit card ending in 7837.²⁸ Investigators reviewed bank surveillance footage from M.T.'s account

²⁷ Check number 8463 was issued for \$2,862.18. However, the ATM deposit receipt notated a deposit of \$2,862.10, which corresponded to BB&T's records of M.T.'s deposit of check 8463 into his account ending in 8840.

²⁸ M.T. maintained an account with BB&T ending in 8840 and a debit card ending in 7837.

provided by BB&T Bank and identified LOGAN, driving a beige Ford Taurus, wearing a gray hooded sweatshirt and red pants, using the drive-through ATM at a BB&T Bank in Richwood, New Jersey. The surveillance footage also showed that LOGAN endorsed the front and the back of the check, as both the check issuer (Joel's Auto Technology) and the intended payee (M.T.). After LOGAN endorsed both sides of the check, he deposited it into M.T.'s account. Investigators confirmed that the fraudulent activity on M.T.'s account, including the time, location, and last four digits of the account number, corresponded to images found in LOGAN's phone.

91. In total, between June 13, 2019, and June 24, 2019, thirteen fraudulent checks totaling \$12,747.56, were deposited into M.T.'s BB&T Bank account. All thirteen checks were issued by various car dealerships including Joel's Auto Technology located in Glassboro, New Jersey, Carney's Auto Center Inc. located in Wenonah, New Jersey, National Collision Co, Inc. located in Philadelphia, Pennsylvania, and Colonial Nissan located in Feasterville, Pennsylvania. BB&T subsequently closed M.T.'s account.

92. Investigators identified several communications beginning on June 11, 2019 on LOGAN's phone between LOGAN and phone number 609-328-4090. Subscriber records obtained by investigators show that this number was subscribed to DEZHON MCCRAE, 3849 South Delsea Drive, in Vineland, New Jersey, with an effective date of February 26, 2019. On June 11, 2019, MCCRAE provided LOGAN with M.T.'s full name, address and financial institution. On June 12, 2019, MCCRAE sent LOGAN a M.T.'s PIN, along with his username (*****r20) and password for online banking.

93. Between June 15, 2019 and June 24, 2019, MCCRAE shared screenshots with LOGAN from BB&T's mobile banking application, displaying an account ending in 8840 and user id ending in r20, both of which correspond to M.T.'s BB&T account. On June 22, 2019, LOGAN sent MCCRAE a

screenshot of an ATM receipt from a withdrawal conducted at a PNC Bank ATM located within a Wawa in Mullica Hill, New Jersey. LOGAN sent the same screenshot to MARTIN on June 26, 2019. This screenshot also had a BB&T debit card, ending in 7837, the same last four digits of M.T.'s debit card, and a stack of cash located behind the debit card with the corresponding receipt from the PNC Bank ATM. Based on M.T.'s bank statements, multiple \$500 withdrawals were conducted at the PNC ATM located within the Wawa in Mullica Hill, New Jersey between June 15 and June 22, 2019.

94. Investigators learned that between June 14, 2019 and June 22, 2019, M.T.'s account was accessed by LOGAN at an ATM in Richwood, New Jersey. M.T.'s debit card was used to purchase over \$5,500.00 worth of USPS money orders that were subsequently deposited by MCCRAE, MCCRAE's girlfriend, and MASSA, at various locations within New Jersey.

k. July 31, 2019 Fraudulent Activity – Victim Goodies Automotive and C.F.-1

95. On July 31, 2019, the Woodbury City Police Department received a report of fraud from Goodies Automotive Services LLC, who suffered a loss of approximately \$3,687.79. Goodies Automotive Services LLC reported that multiple fraudulent business checks were mobile deposited by four different unknown individuals on her/his Fulton Bank business account. Investigators identified thirty-four fraudulent business checks, totaling approximately \$15,005.88, drawn from Goodies Automotive Services LLC business account, that were mobile deposited or attempted to be deposited into approximately 6 different bank accounts. Investigators found that between July 15, and July 18, 2019, approximately thirteen of the business checks were mobile deposited into a TD Bank account of an individual identified herein as "C.F.-1."

96. Investigators interviewed C.F.-1 who told them that he/she responded to a social media advertisement on Instagram to "make quick money" posted by "Kayg0ldi," known to C.F.-1 as a female

named Kayla. C.F.-1 told investigators he/she initially spoke with “Kayg0ldi” via direct message on Instagram, excerpts of which are attached hereto as “Exhibit 12.”

97. C.F.-1 told investigators that he/she subsequently communicated with MASSA through texts using phone number 609-592-2813. In those texts MASSA instructed him/her to meet MASSA at the Wawa in Egg Harbor Township, New Jersey and hand over his/her TD Bank information, including his/her debit card, PIN, and online bank account information. On or about July 12, 2019, C.F.-1 met MASSA at the Wawa in Egg Harbor Township, New Jersey, and gave MASSA all the requested bank information. According to C.F., MASSA explained that after her “business partner” received funds, they would split the money three ways. C.F.-1 stated that he/she never received any money and eventually realized he/she was unwittingly involved in a fraud scheme. C.F.-1 told investigators that he/she watched as the funds in his/her account increased and decreased and he/she began receiving ATM fees and overdraft fees. C.F.-1 contacted MASSA and told her that he/she would report her to the police. C.F.-1 said that MASSA told him/her, “Do what you gotta do.”

98. Investigators reviewed C.F.-1’s TD Bank checking account statements and identified eleven mobile deposits, totaling approximately \$3,531.14, between July 12, 2019 and July 19, 2019. From approximately July 15, 2019 through July 21, 2019, C.F.-1’s debit card was used in multiple ATM withdrawals at various Wawa locations in New Jersey including Bellmawr, Pennsauken, Sewell and Mullica Hill, totaling approximately \$1,660.00.²⁹ During that same time period, C.F.-1’s debit card was used in multiple businesses including English Creek Car Wash in Egg Harbor, New Jersey and a parking facility in Miami Beach, Florida.³⁰ The eleven checks deposited into C.F.-1’s account were deemed to

²⁹ Total does not include non TD Bank ATM fees or other transactions fees such as balance inquiry fees.

³⁰ There were multiple online transfer between accounts as well as at least one automated debit from C.F.-1’s account not reflected in the above activity.

be fraudulent and returned. In September, 2019, C.F.-1's TD Bank account with negative balance of \$2,873.77.

k. August 2, 2019 Fraudulent Activity – Victim Route 33 Nissan

99. On August 2, 2019, Republic Bank contacted investigators regarding a fraudulent Route 33 Nissan check deposited into a newly opened³¹ Republic Bank account belonging to N.C. The check, issued for \$2,418.67, was drawn from Route 33³² Nissan's Valley National bank account and deposited at the Republic Bank ATM in Sewell, New Jersey on or about August 1, 2019. Investigators reviewed the surveillance images provided by Republic Bank for this deposit, which depicted a black male with short black hair wearing a bright green hooded sweatshirt. Investigators identified MARTIN as the depositor based upon the matching physical description and attire previously identified by investigators during a review of social media. Republic Bank advised an initial attempt was conducted on July 31, 2019, at a drive through Republic Bank ATM in Media, Pennsylvania. Because a wrong PIN number was utilized, the deposit was rejected. However, Republic Bank captured surveillance footage of this attempt, which identified a white Nissan Altima bearing New Jersey registration H30-LCC. Based upon registration information, the registrant of the vehicle was Just Four Wheels, Inc., a vehicle rental company, located in Galloway, New Jersey. Investigators contacted Just Four Wheels Inc., and learned that the vehicle was rented by HAINES during this time frame. Just Four Wheels Inc., also advised they maintain a satellite office at Nissan Woodbury. Just Four Wheels Inc. provided a copy of the rental contract; the rental location corresponded to Nissan Woodbury's listed address. Republic Bank suffered

³¹ Account was opened on approximately July 16, 2019 with \$60.00 cash, which was withdrawn the following day via ATM.

³² In the communication between LOGAN and HAINES, investigators identified a Route 33 Nissan check, with the same routing and account number as the fraudulent checks, legitimately issued to Woodbury Nissan, as referenced in paragraph 89.

no loss as N.C.'s account was restricted after the August 1, 2019 deposit, despite an attempt to withdraw \$500.00 on August 2, 2019 at an ATM located inside a Wawa in Mount Laurel, New Jersey.

100. Investigators identified communication between LOGAN and MARTIN, illustrating MARTIN's knowledge and involvement in the fraud scheme.³³ Specifically, on June 26, 2019, MARTIN sent LOGAN a message with victim "R.P.'s" details, including his/her date of birth and address. On the same date, MARTIN sent LOGAN another message with victim "H.T."s details, to include his/her date of birth and address. This information is consistent with logging into third party bank accounts for the purposes of facilitating the fraud scheme. R.P.'s debit card and a check issued to H.J.³⁴, were recovered inside MASSA's Gold Ford, which was occupied by LOGAN, FELICIANO, and MARTIN, during the vehicle stop in Glassboro, New Jersey on June 28, 2019. Investigators identified three USPS purchases conducted on June 28, 2019, utilizing R.P.'s debit card, the receipt for one of which was also recovered during the vehicle stop, for the purchase of money order 25597529291. This money order and two additional USPS money orders,³⁵ also purchased with R.P.'s debit card, were recovered in MASSA's Gold Ford. Additionally, investigators recovered the "Customer's Receipt" portion of a USPS money order bearing serial number 25694743950, purchased at the Clayton Post Office on May 24, 2019.³⁶ Investigators retrieved the purchase information for this money order and identified another USPS money order was purchased during the same transaction. Both USPS money

³³ Investigators reviewed data extracted from both LOGAN and MARTIN's phones, both of which were seized during the car stop on June 28, 2019 in Glassboro, referenced in paragraphs 81 and 82.

³⁴ The check was purported to be issued by Joden World Resources LLC for \$1,105.19.

³⁵ USPS money order 25694748696 and 25926958956 – all 3 USPS money orders are currently logged as evidence at Glassboro Police Department.

³⁶ Every USPS money order issued has a perforated top portion, titled "Customer's Receipt" which details the USPS serial number purchased along with the transaction date, post office, amount, and issuing clerk.

orders were redeemed by MCCRAE, one on May 28, 2019, at the Glassboro Post Office and the other redeemed on June 5, 2019, at the Clayton Post Office.

l. September 4, 2019 Fraudulent Activity – Factory Tune Automotive Inc.

101. On or about August 31, 2019, MARTIN posted a story on his Instagram account, 1hunnit_mill, which depicted a hand holding a small jar of vegetation, suspected to be marijuana. Below the hand, a business check was visible. A still shot of the story depicted the business check contained a partial view of the payer, “ctory Tune Automotive, Inc.,” with an address listed on the Black Horse Pike. From this information, investigators identified the business as Factory Tune Automotive with a listed address of 1321 N Black Horse Pike, Williamstown, New Jersey. A zoomed-in image of the original image is attached hereto as “Exhibit 13.”

102. Investigators contacted Factory Tune Automotive Inc., who confirmed eight fraudulent checks, totally approximately \$15,670.47, were drawn off of their business account. Factory Tune Automotive provided investigators copies of the fraudulent checks. Investigators identified another fraudulent Factory Tune Automotive check, check number 1951, issued for \$3,479.22, which was deposited into a newly opened Republic Bank account belonging to individual K.H. Republic Bank advised K.H.’s account was opened on August 30, 2019 with an initial deposit of \$30.00. On or about September 4, 2019, the fraudulent Factory Tune Automotive check was deposited into K.H.’s account through a Republic Bank ATM, located in Philadelphia, Pennsylvania. Surveillance footage obtained from the ATM deposit depicted LOGAN conducting the transaction.

m. September 25, 2019 Fraudulent Activity – Victim Campus Crossings Apartments

103. On September 25, 2019, Glassboro Police Department received a report of fraud from Campus Crossings Apartments located in Glassboro, New Jersey. Campus Crossings Apartments reported that two fraudulent checks, drawn of their business bank account, were deposited into two

separate accounts, totaling approximately \$2,891.02. The first check, check number 5279, issued for \$1,948.61, was deposited into N.P.'s Republic bank account, with "The Crossings at Glassboro LLC" listed on the check as the payer. This fraudulent check was deposited into N.P.'s account by FELICIANO on September 11, 2019 at a Republic Bank ATM located in Voorhees, New Jersey. Republic Bank fraud investigators identified several attempts to transfer funds from N.P.'s bank account to a Cash App account under the user name "Halle Allen," but all attempts were rejected.

104. The second check, check number 5281, issued for \$942.41, to individual S.D., was cashed at Fairwinds Credit Union on or about September 12, 2019 in Orlando, Florida. This check was drawn off of Campus Crossing Apartments' TD bank account but the fraudulent check had the listed payer as "Copley Property Preservation LLC."³⁷

105. Investigators confirmed that both MASSA and LEIRE were residents of Campus Crossings Apartments until their lease ended on July 31, 2019. Campus Crossings Apartments issued LEIRE check number 5266 for \$1,194.03, on approximately August 27, 2019, for the security deposit return. Campus Crossings Apartments mailed the check to the address LEIRE provided, 211 Kinsley Road, Pemberton, New Jersey.³⁸ Campus Crossings Apartments provided investigators with a copy of the check issued to LEIRE, specifically check number 5266, which contained the same bank account number, routing number, address, and other markings observed on the fraudulent checks. TD Bank representatives said that this check was deposited into a Citibank account, which investigators later identified belonged to LEIRE's mother, Kylene Medina.

³⁷ During the course of this investigation, investigators identified various instances where the information for the listed payer imprinted on the fraudulent checks did not correspond to the routing and account number also imprinted on the checks. This was purposely done to conceal the true victims and the corresponding compromised bank accounts.

³⁸ Investigators confirmed this is an address associated with the MASSA family.

106. Throughout the course of this investigation, investigators reviewed individual and business bank records, identified fraudulent check deposits as well as fraudulent/stolen USPS and Western Union money orders, and conducted interviews with individuals and businesses associated to the fraudulent activity. Investigators located and reviewed approximately 1,238 fraudulent checks, with an intended loss at or around \$514,033.00. Western Union provided investigators with approximately five-hundred ninety-nine fraudulent money orders, all of which originated from the same check cashing location in New York and within the same serial number blocks. Four-hundred and six of these were deposited into bank accounts, for an estimated intended loss of approximately \$471,790.00. USPS identified fifty-three money orders stolen from the Berlin Post Office, thirty of which were deposited into various bank accounts, for an estimated loss exposure of \$29,840.00. Based on the accounts reviewed and the fraudulent activity identified, investigators estimate the total intended loss to be at least \$1,015,663.00.

107. Based on a review of bank records, interviews conducted with victims, USPS records and through routine collection of social media data, there is probable cause to believe that MASSA, HERRIN, FELICIANO, LOGAN, MCCRAE, LEIRE, HAINES, MCDANIELS, MARTIN, JOHNSON, and other co-conspirators known and unknown, conspired together and with others to commit the Specified Federal Offenses outlined in this affidavit.

Exhibit 1

(MASSA Advertisements)

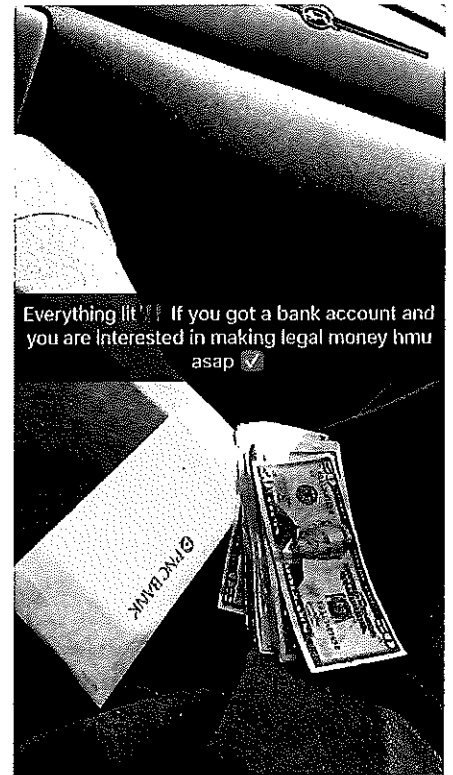
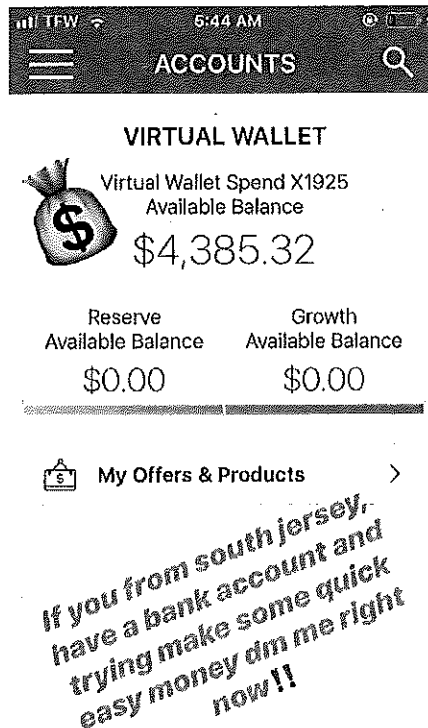
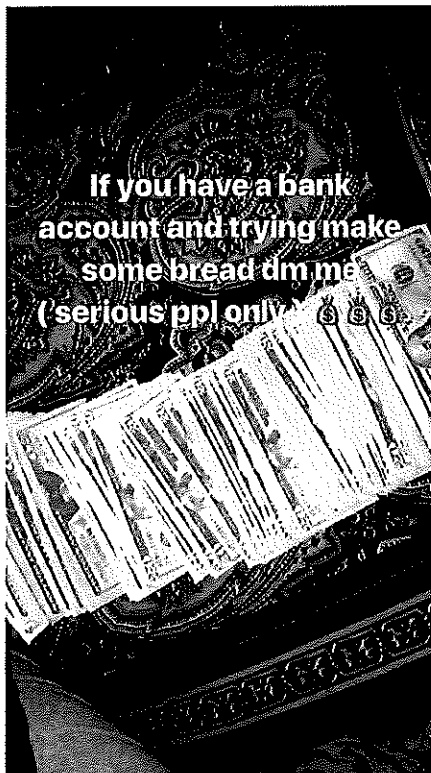
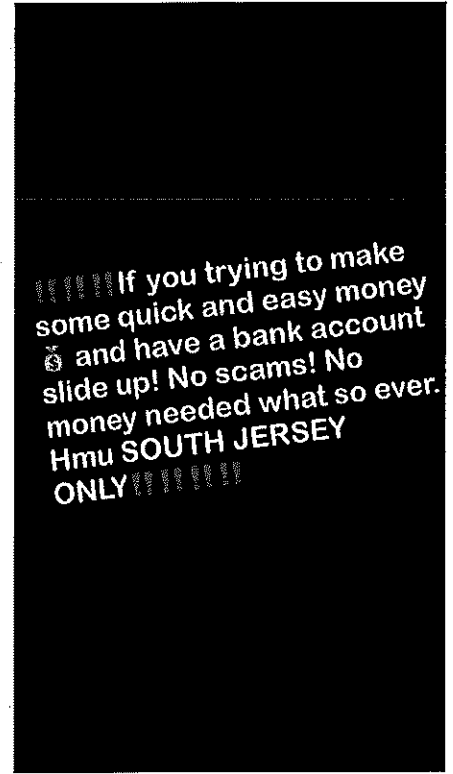


Exhibit 2

(LOGAN's Advertisements)

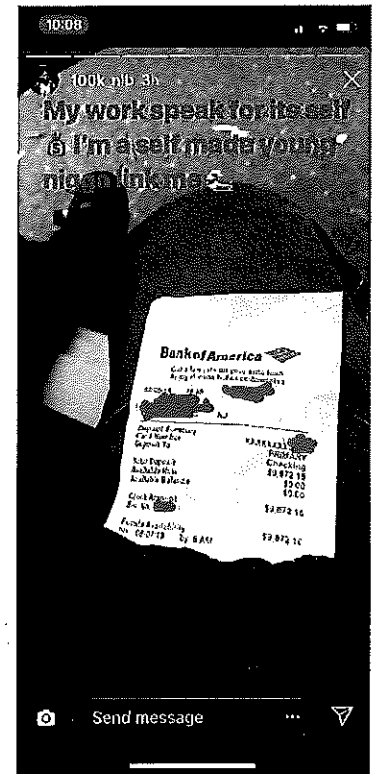
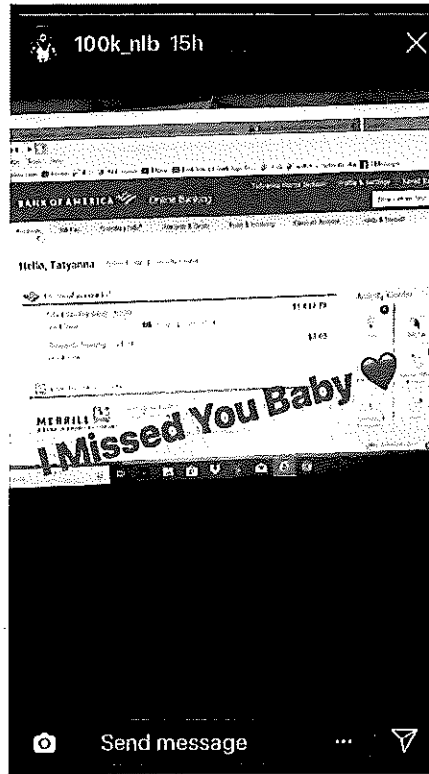


Exhibit 3

(MCCRAE Advertisements)

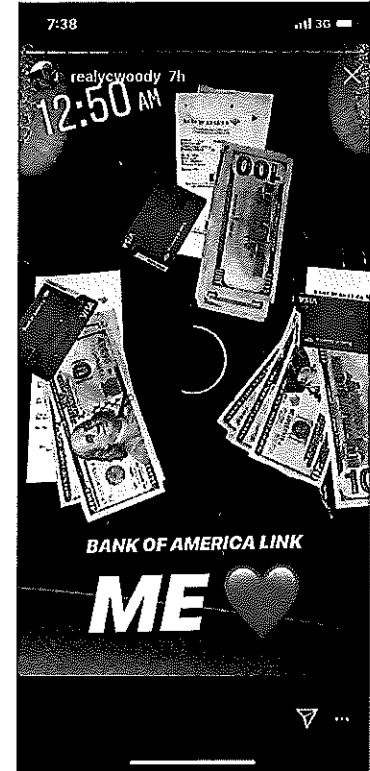
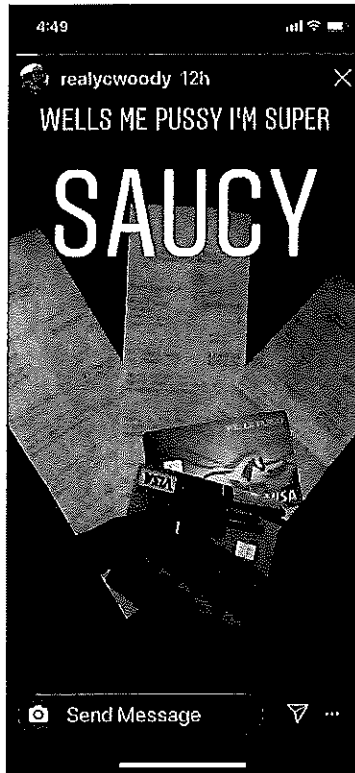


Exhibit 4

(LEIRE Advertisements)

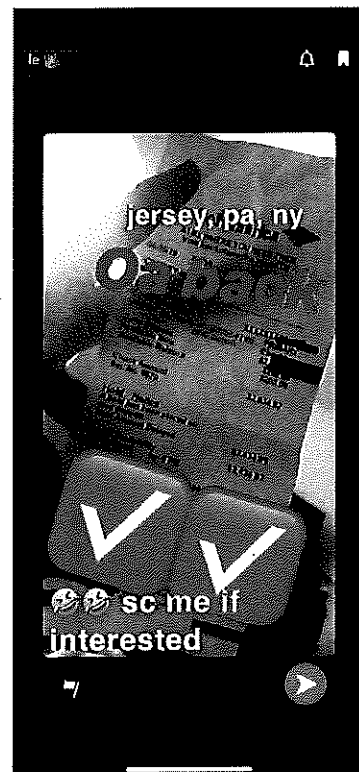
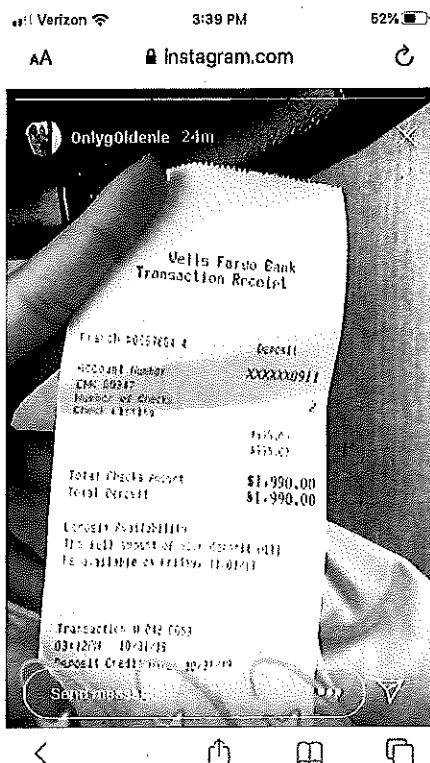
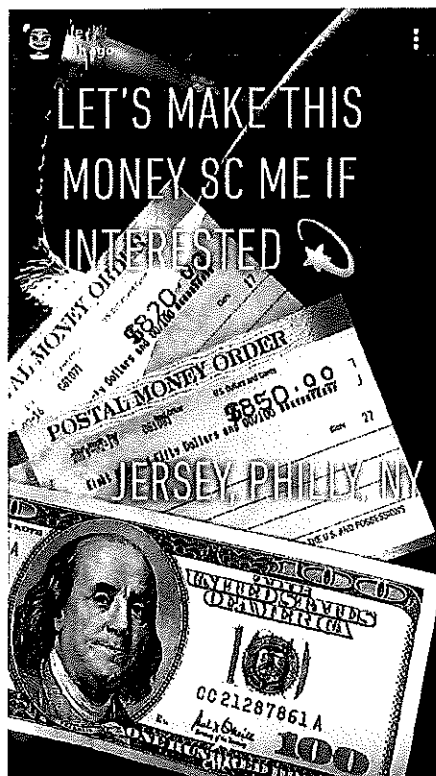


Exhibit 5

(JOHNSON's Advertisements)

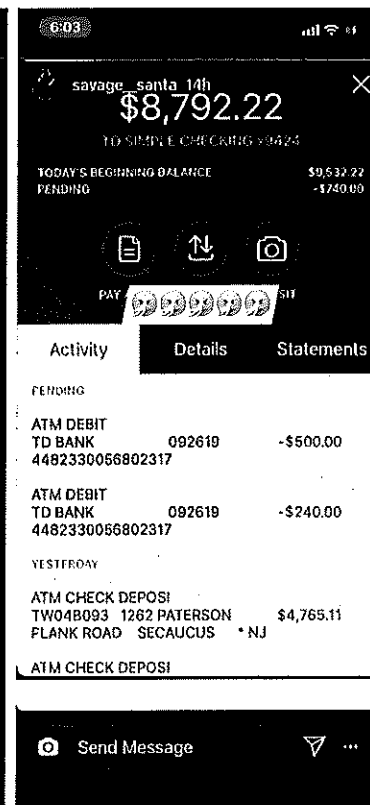
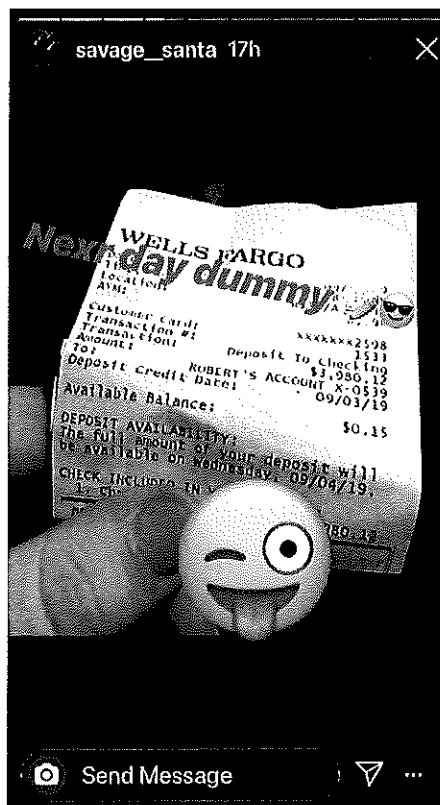
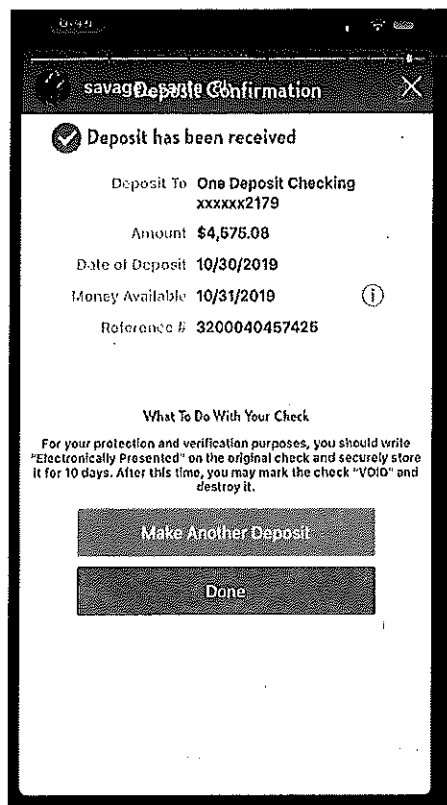


Exhibit 6

(HAINES' Advertisements)

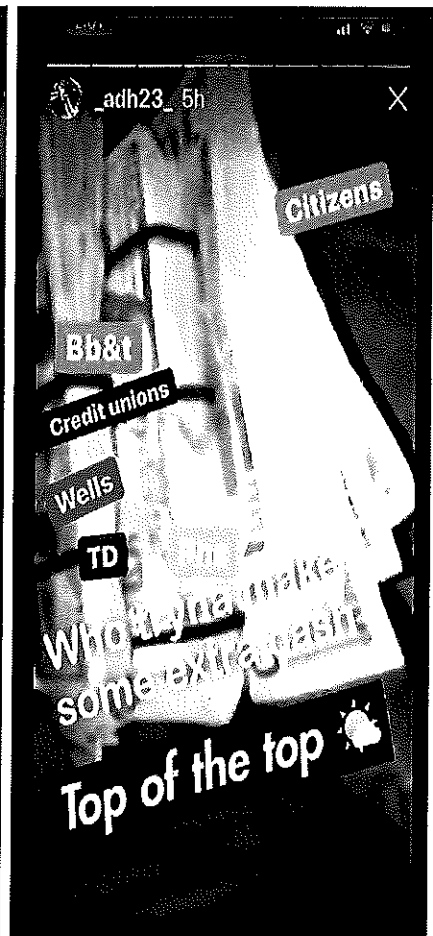
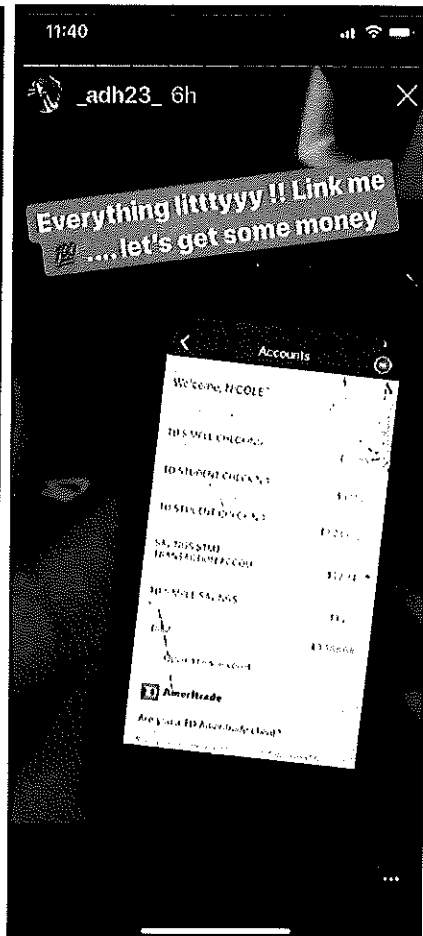
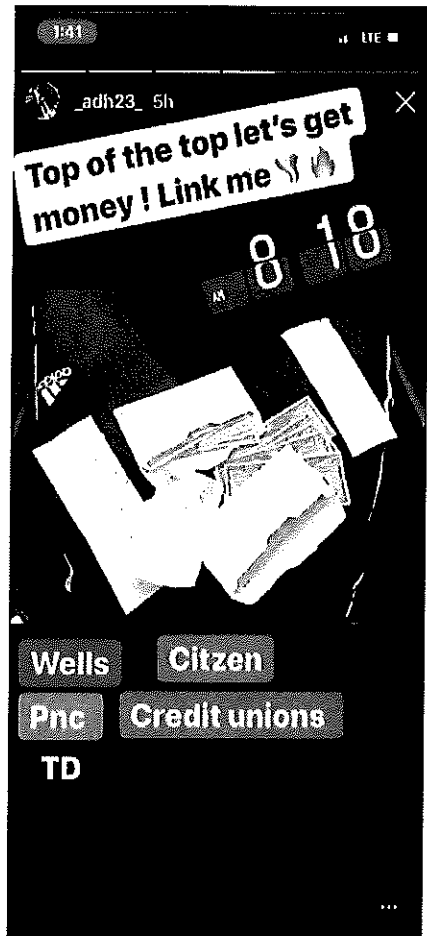


Exhibit 7

(MARTIN's Advertisements)

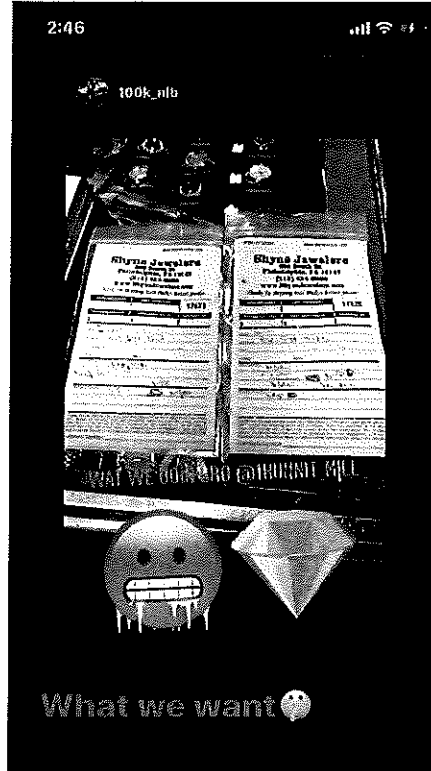
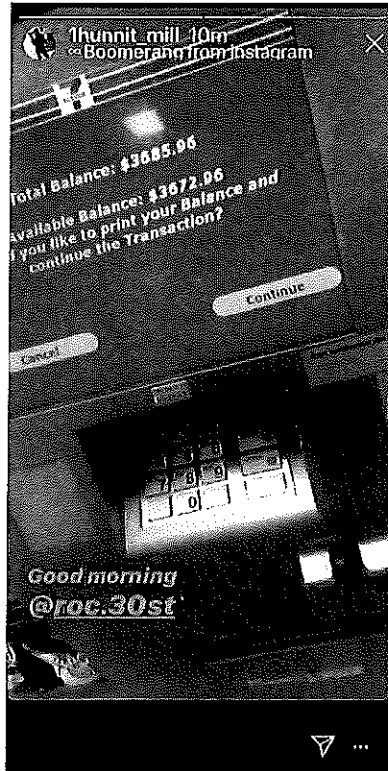


Exhibit 8

(MCDANIELS' Advertisements)

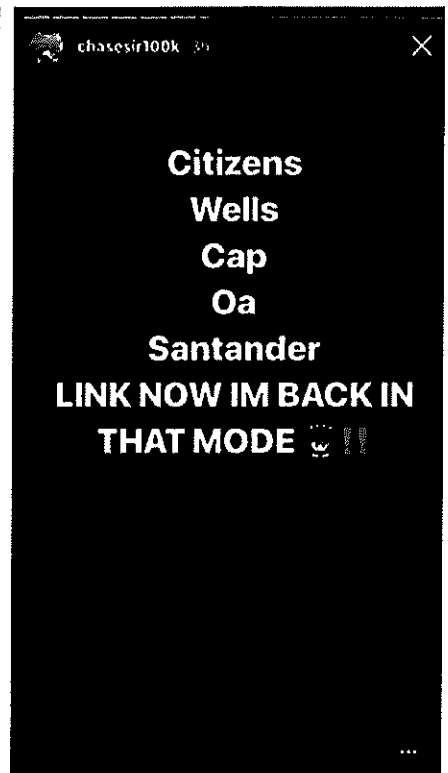
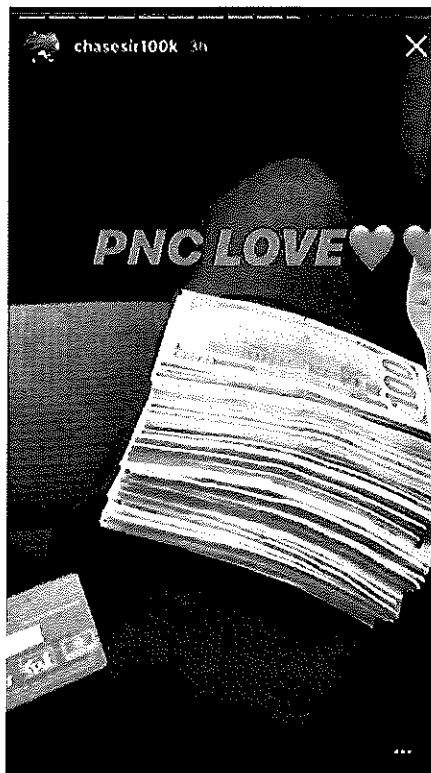


Exhibit 9

(MASSA and A.S. text exchange)

1

6:58 AM

kay.fckng0ldi

KAY.FCKNG0LDI:
Where you located

ME:
blackwood

KAY.FCKNG0LDI:
Who you bank with?

ME:
Bank of america

KAY.FCKNG0LDI:
How long you had it?

ME:
You know the process? Wanna make \$500.2k by tomorrow?

KAY.FCKNG0LDI:
I don't know the process but like for 3 years already.

KAY.FCKNG0LDI:
It's basically small checks getting deposit into your account. From a payroll called fine wine so it's legit. You get half of what I got so anywhere from \$500.2k

ME:
Bett

KAY.FCKNG0LDI:
I would need your online banking and pin. The

2

6:58 AM

kay.fckng0ldi

online banking is to make sure it's secure and process the correct way
And we would have to meet up for the actual card if you have any other questions feel free to ask me.

ME:
ard

KAY.FCKNG0LDI:
Can we meet today?
I'm from pine hill

ME:
Im home rn in blackwood but ik codes but yeah
& my online banking pin? like my 4 digit code.

KAY.FCKNG0LDI:
I can come now?

ME:
yeah. you just need my pin right?

KAY.FCKNG0LDI:
And yea your user, pass & pin
What's your # and addy

ME:
lmao damn ok
I got bank of america
so it's

3

6:58 AM

kay.fckng0ldi

Which is the pass

ME:
0622
I mean Loxy0427 lmao

KAY.FCKNG0LDI:
Lmao it's ok babe what's your addy
I'm about to come in like 10-15 mins

ME:
ard, you don't need my card correct

KAY.FCKNG0LDI:
Yes I do babe that's how the Atm deposit is made but you will have it back by tm

ME:
ard.

KAY.FCKNG0LDI:
You have to also be up at 3am & at 8am

ME:
That's cool?

KAY.FCKNG0LDI:
lmao omg yeah

KAY.FCKNG0LDI:
Sorry ts

4

6:59 AM

kay.fckng0ldi

okay

KAY.FCKNG0LDI:
And I need your security questions as well if you have it set up

ME:
damn ion remember that
lmc if I can get it

KAY.FCKNG0LDI:
Ok babe try to remember
And last thing I need is your last 4 ssn

ME:
I just texted you
Can you call and raise your atm limit to 2500

KAY.FCKNG0LDI:
The question it's gon ask if my first pet name, answer is "oreo"
and yeah lmc

KAY.FCKNG0LDI:
Is there any more questions and ok thanks babe

ME:
no i trust you

Exhibit 10

(LEIRE's Snapchat Advertisement Featuring US Postal Money Orders)

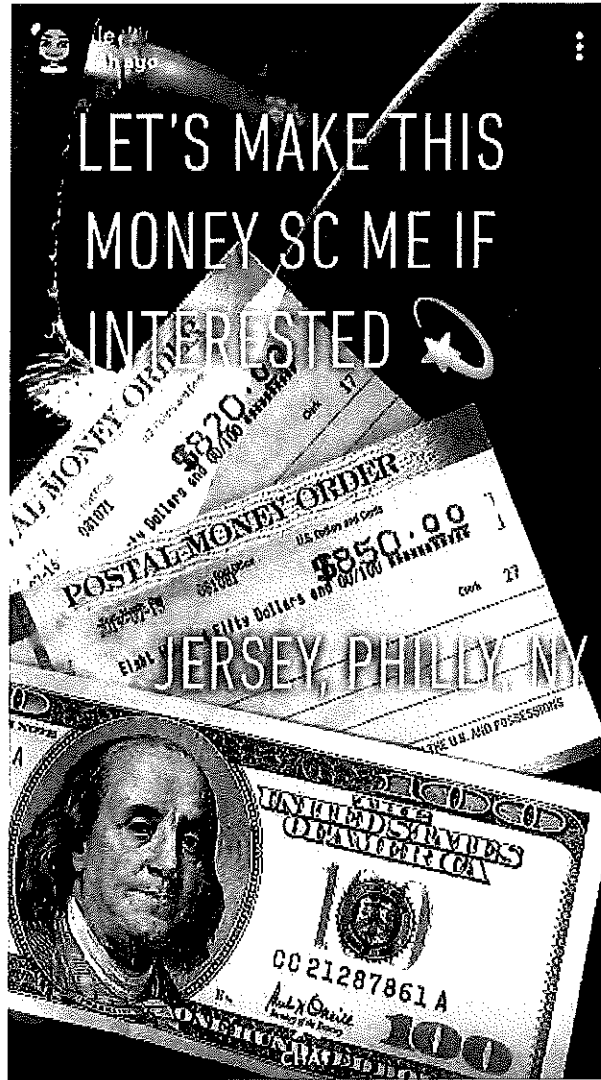


Exhibit 11

(MASSA and M.H. Instagram direct messenger exchange)

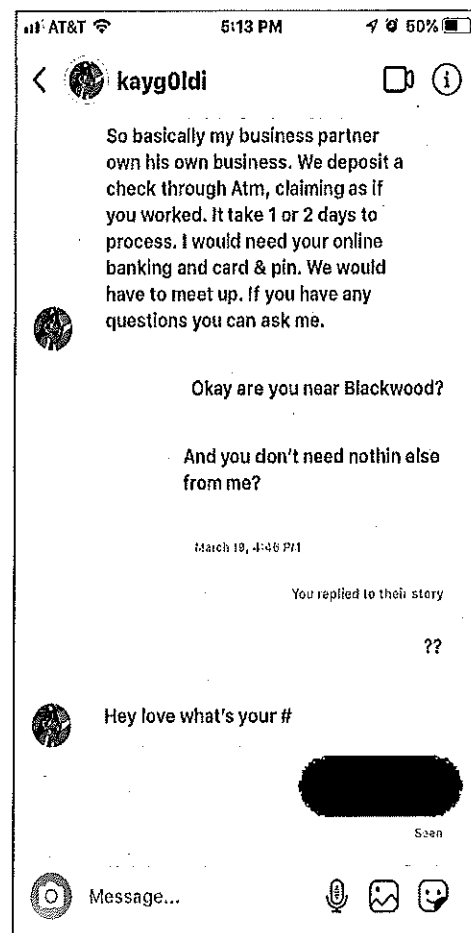
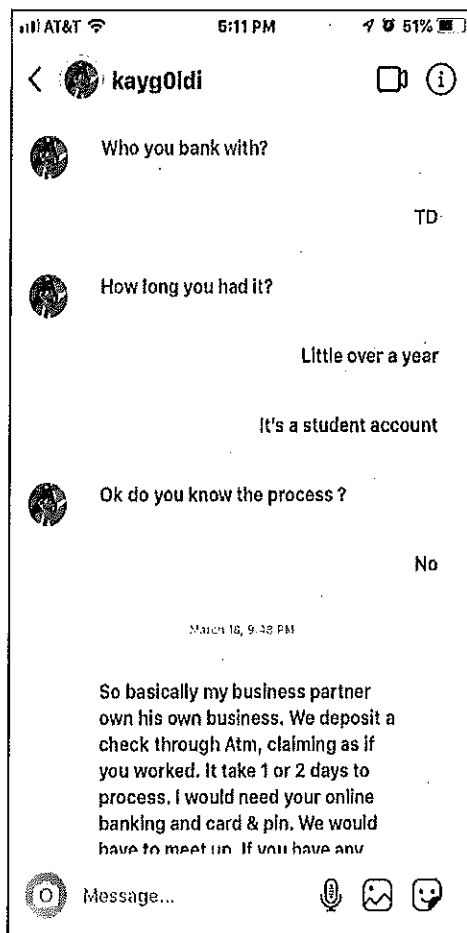
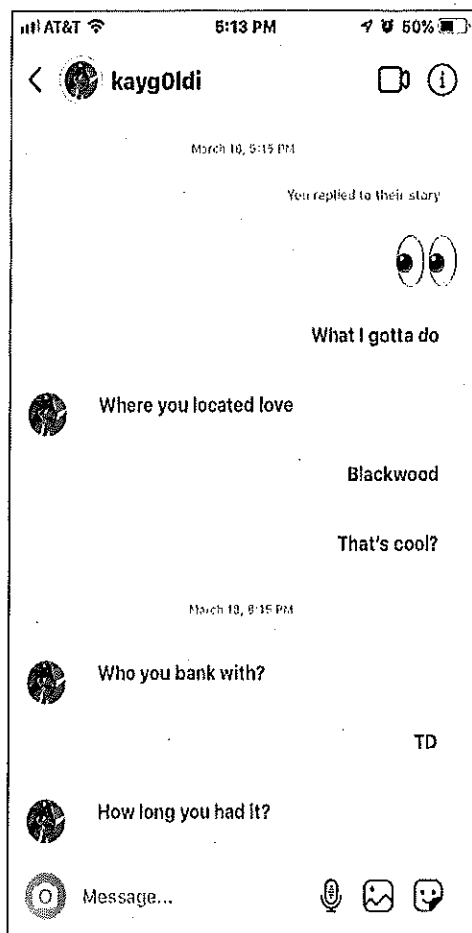


Exhibit 12

(MASSA's conversation with C.F.-1)

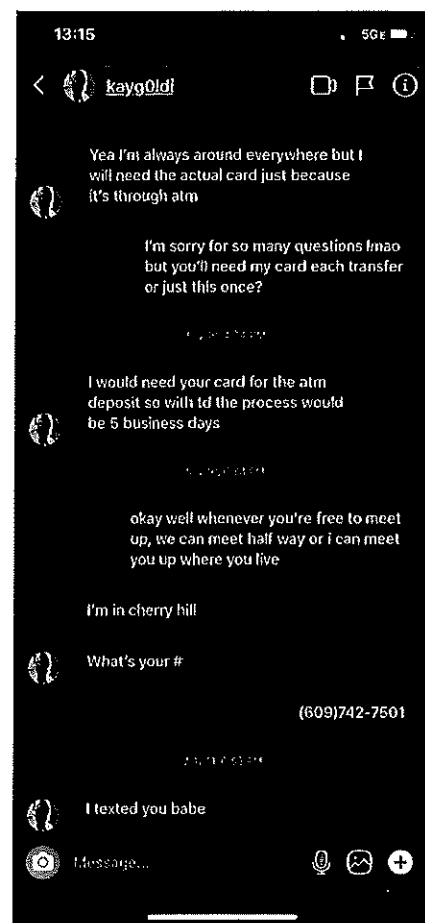
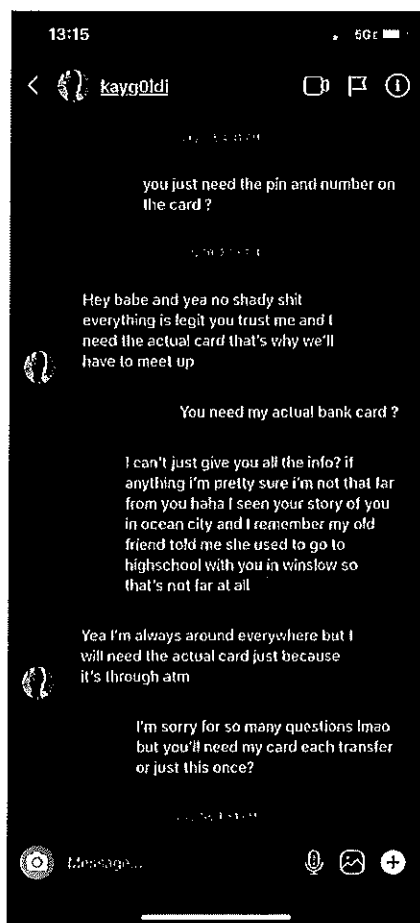
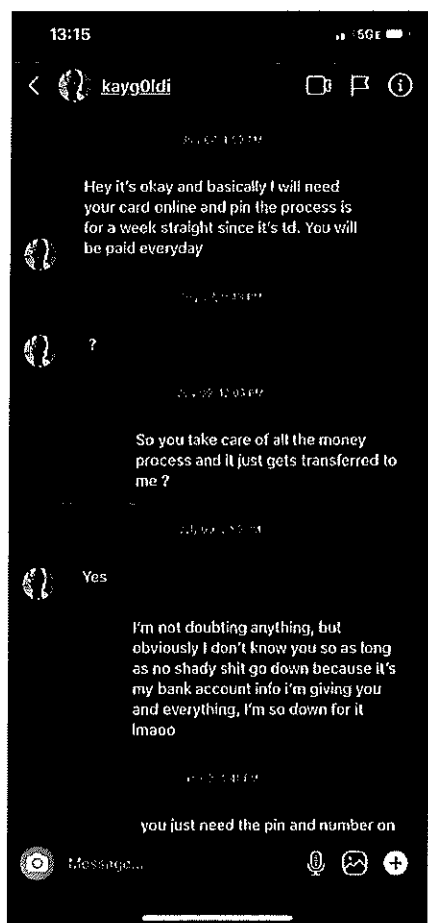


Exhibit 13

(MARTIN's image with "Factory Tune Automotive Inc." check zoomed-in)

