

ORIGINAL

17 MAG 8785
Sheb Swett

Approved: Sheb Swett
SHEB SWETT/NOAH SOLOWIEJCZYK
Assistant United States Attorneys

Before: THE HONORABLE DEBRA FREEMAN
United States Chief Magistrate Judge
Southern District of New York

----- X

SEALED
COMPLAINT

UNITED STATES OF AMERICA

- v. -

Violations of
18 U.S.C. §§ 1349,
1029(b)(2), 1028A

LOUIS PINA,
MALIK GRAY,
GEORGE JOSEPH,
AKEEM KRUBALLY,
THERESA OUTERBRIDGE,
DEVON WILLIAMS,
HAKEEM BALDEO,
QUINTEEN LYNCH,
KHALID NAZZAL,
FRANCISCO VIRUET, and
JOHNNY SERRANO,

COUNTY OF OFFENSE:
BRONX

Defendants.

----- X

SOUTHERN DISTRICT OF NEW YORK, ss.:

ANTHONY GIATTINO, being duly sworn, deposes and says that he is a Criminal Investigator with the United States Attorney's Office for the Southern District of New York, and charges as follows:

COUNT ONE

(Conspiracy to Commit Wire Fraud)

1. From at least in or about October 2016, up to and including at least in or about October 2017, in the Southern District of New York and elsewhere, LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, AKEEM KRUBALLY, THERESA OUTERBRIDGE, DEVON WILLIAMS, HAKEEM BALDEO, QUINTEEN LYNCH, KHALID NAZZAL, FRANCISCO VIRUET, and JOHNNY SERRANO, the defendants, and others

known and unknown, willfully and knowingly did combine, conspire, confederate, and agree together and with each other to commit wire fraud, in violation of Title 18, United States Code, Section 1343.

2. It was a part and object of the conspiracy that LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, AKEEM KRUBALLY, THERESA OUTERBRIDGE, DEVON WILLIAMS, HAKEEM BALDEO, QUINTEEN LYNCH, KHALID NAZZAL, FRANCISCO VIRUET, and JOHNNY SERRANO, the defendants, and others known and unknown, willfully and knowingly, having devised and intending to devise a scheme and artifice to defraud and for obtaining money and property by means of false and fraudulent pretenses, representations, and promises, would and did transmit and cause to be transmitted by means of wire, radio, and television communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds for the purpose of executing such scheme and artifice, in violation of Title 18, United States Code, Section 1343.

(Title 18, United States Code, Section 1349.)

COUNT TWO

(Access Device Fraud Conspiracy)

3. From at least in or about October 2016, up to and including at least in or about October 2017, in the Southern District of New York and elsewhere, LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, AKEEM KRUBALLY, THERESA OUTERBRIDGE, DEVON WILLIAMS, HAKEEM BALDEO, QUINTEEN LYNCH, KHALID NAZZAL, FRANCISCO VIRUET, and JOHNNY SERRANO, the defendants, and others known and unknown, knowingly did combine, conspire, confederate, and agree together and with each other to commit access device fraud, in violation of Title 18, United States Code, Sections 1029(a)(2), (a)(3), and (a)(5).

4. It was a part and an object of the conspiracy that LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, AKEEM KRUBALLY, THERESA OUTERBRIDGE, DEVON WILLIAMS, HAKEEM BALDEO, QUINTEEN LYNCH, KHALID NAZZAL, FRANCISCO VIRUET, and JOHNNY SERRANO, the defendants, and others known and unknown, knowingly, and with intent to defraud, and affecting interstate and foreign commerce, would and did produce, use, and traffic in one and more unauthorized access devices during a one-year period, and by such conduct would and did obtain things of value aggregating \$1,000 and more during that period, in violation of Title 18, United States Code, Section 1029(a)(2).

5. It was further a part and an object of the conspiracy that LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, AKEEM KRUBALLY, THERESA OUTERBRIDGE, DEVON WILLIAMS, HAKEEM BALDEO, QUINTEEN LYNCH, KHALID NAZZAL, FRANCISCO VIRUET, and JOHNNY SERRANO, the defendants, and others known and unknown, knowingly, and with intent to defraud, and affecting interstate and foreign commerce, would and did possess fifteen and more devices which were counterfeit and unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(3).

6. It was further a part and an object of the conspiracy that LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, AKEEM KRUBALLY, THERESA OUTERBRIDGE, DEVON WILLIAMS, HAKEEM BALDEO, QUINTEEN LYNCH, KHALID NAZZAL, FRANCISCO VIRUET, and JOHNNY SERRANO, the defendants, and others known and unknown, knowingly, and with intent to defraud, and affecting interstate and foreign commerce, effected transactions with 1 and more access devices issued to other persons, to receive payment and any other thing of value during a one-year period, the aggregate value of which was equal to and greater than \$1,000, in violation of Title 18, United States Code, Section 1029(a)(5).

OVERT ACTS

7. In furtherance of the conspiracy and to effect the illegal objects thereof, the following overt acts, among others, were committed in the Southern District of New York and elsewhere:

a. On or about November 8, 2016, a phone number associated with HAKEEM BALDEO, the defendant, was used to place telephone calls to ride-sharing drivers in order to obtain information used to obtain unauthorized access to accounts belonging to those ride-sharing drivers.

b. On or about November 14, 2016, THERESA OUTERBRIDGE, the defendant, received funds that had been obtained through unauthorized access to an account belonging to a ride-sharing driver.

c. On or about December 5, 2016, AKEEM KRUBALLY, the defendant, provided GEORGE JOSEPH, the defendant, information for a bank account, which, on or about December 12, 2016, was used to receive a deposit of approximately \$1,283.16 that had been stolen from an account belonging to a driver of a ride-sharing company.

d. On or about January 10, 2017, LOUIS PINA, the defendant, sent MALIK GRAY, the defendant, a Snapchat message containing bank account information for FRANCISCO VIRUET, the defendant, which was later used to receive a deposit totaling \$753.13 that had been obtained through the unauthorized use of an access device belonging to a ride-sharing driver.

e. On or about January 15, 2017 and on or about January 17, 2017, DEVON WILLIAMS, the defendant, used a cellular telephone device to obtain unauthorized access to accounts belonging to drivers of a ride-sharing company, which resulted in the unauthorized transfer of funds to QUINTEEN LYNCH, the defendant.

f. On or about February 4, 2017, members of the conspiracy logged into the account of a ride-sharing driver without authorization, and changed the bank account information for the driver such that approximately \$1,150.65 was transferred from the ride-sharing driver's account to JOHNNY SERRANO, the defendant, among others.

g. On or about April 3, 2017, KHALID NAZZAL, the defendant, received funds that had been obtained through the unauthorized access to an account belonging to a ride-sharing driver.

(Title 18, United States Code, 1029(b)(2).)

COUNT THREE

(Aggravated Identity Theft)

8. From at least in or about October 2016, up to and including at least in or about October 2017, in the Southern District of New York and elsewhere, LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, AKEEM KRUBALLY, THERESA OUTERBRIDGE, DEVON WILLIAMS, HAKEEM BALDEO, QUINTEEN LYNCH, KHALID NAZZAL, FRANCISCO VIRUET, and JOHNNY SERRANO, the defendants, knowingly did transfer, possess, and use, without lawful authority, a means of identification of another person, during and in relation to a felony violation enumerated in Title 18, United States Code, Section 1028A(c), to wit, without authorization, the defendants used, and aided and abetted the use of, the names, phone numbers, email addresses, driver's license numbers, and unique passwords, belonging to other individuals during and in relation to the felony violation charged in Count One of this Complaint.

(Title 18, United States Code, Sections 1028A(a)(1),
1028A(c)(5), and 2.)

The bases for my knowledge and for the foregoing charges are, in part, as follows:

9. I am a Criminal Investigator with the United States Attorney's Office for the Southern District of New York and I have been personally involved in the investigation of this matter. I have worked on this investigation with Special Agents from the United States Secret Service ("USSS") as well as criminal investigators with the Westchester County District Attorney's Office ("WCDAO"). This affidavit is based upon my investigation, my conversations with witnesses and other law enforcement agents, and my review of documents and records obtained in the course of this investigation. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

Overview of the Scheme

10. From my participation in this investigation, I know that since at least October 2016, a group of individuals operating predominantly in the Bronx and Mount Vernon, New York, have been engaged in a scheme to defraud livery drivers and ride-sharing companies using mobile ride-sharing applications (the "Scheme").¹ As set forth in greater detail below, the Scheme has targeted drivers associated with two ride-sharing companies ("Company-1" and "Company-2"). Scheme members call Company-1 and Company-2 drivers, posing as Company-1 and Company-2 representatives. During these conversations, Scheme members obtain unique personal identifiers and other information through deception and social engineering, generally by pretending to be an employee of Company-1 or Company-2. Then, Scheme members use that information to obtain unauthorized access into the online Company-1 and Company-2 driver accounts,

¹ "Ride-sharing," as used in this Complaint, refers to a business model in which companies connect livery drivers to customers for one-time rides on short notice. These companies use mobile applications as the platform for both riders and drivers.

and alter information in those compromised accounts to divert driver funds to bank accounts controlled by Scheme members.

Overview of the Company-1 Scheme

11. Based on my conversations with representatives from a Company-1, as well as my review of documents provided by Company-1, I have learned that the Scheme typically operates as follows with respect to Company-1:

a. When an individual orders a ride through Company-1's mobile application ("App-1"), Company-1 provides the individual with information about the driver, including the driver's name, picture, and an anonymized phone number so that the rider can communicate with the driver.

b. When a driver logs into App-1, he or she enters his or her phone number during the login process. Company-1 then employs multiple security measures to ensure that the driver is the authorized user of the account. Among other things, during the login process, Company-1 automatically sends a text message containing a unique code to the phone number associated with the driver's account. This unique code can be used to access the account. Further, if the driver attempts to log into App-1 from an unrecognized device, the driver is required to enter his or her driver's license number as well.

c. The fraud scheme involves a Scheme member ordering a ride through App-1 and then cancelling the ride once he or she receives the driver's anonymized phone number. A Scheme member then uses the anonymized phone number to call the driver, and impersonates a representative from Company-1. During the course of the telephone conversation with the driver, the Scheme member asks the driver for the driver's real telephone number.

d. After obtaining the real telephone number of the driver, and while remaining on the phone with the driver, a Scheme member attempts to log into the driver's Company-1 account, which, as discussed above, causes Company-1 to send a text message containing a unique code to the victim driver's cellphone. The Scheme member that is impersonating the representative of Company-1 then attempts to trick the victim driver into providing the unique authentication code that he or she just received, as well as his or her driver's license number.

e. Utilizing the unique code, the victim driver's telephone number, and the victim driver's license number, Scheme members thereafter log into the victim driver's account through App-1 or the Company-1 web interface without the driver's authorization using the victim driver's phone number, unique code, and driver's license number. Once the Scheme member has logged into the victim driver's account, the Scheme Member then proceeds to change the bank account information associated with the account to a bank account that either they or another Scheme member control.

f. As a result of the above-described scheme, funds that the victim driver earned from Company-1 are diverted instead to a Scheme member's bank account. Company-1 generally only sends payment to drivers' designated bank accounts on approximately a weekly basis such that it could take a number of days before a victim driver would realize that the bank account information associated with the driver's Company-1 account had been changed without the driver's authorization.

12. In connection with this investigation, Company-1 has provided law enforcement with a significant amount of data regarding the Scheme. The data provided by Company-1 includes, among other things: (i) information identifying unauthorized accesses to victim driver accounts and unauthorized transfers of funds from those accounts; (ii) the telephone numbers used to call the drivers immediately prior to the unauthorized access of the drivers' Company-1 accounts by Scheme members and the date and time of such telephone calls; (iii) the Internet Protocol ("IP")² addresses used for the unauthorized login to the drivers' Company-1 accounts by Scheme members, during which login session the drivers' bank account information associated with their Company-1 accounts was changed and the date and time of the unauthorized logins; and (iv) unique Apple advertising

² Based on my training and experience, I have learned that every computer or device on the Internet is referenced by a unique IP Address the same way every telephone has a unique telephone number. An IP Address is a series of four numbers separated by a period, and each number is a whole number between 0 and 254. Each time an individual accesses the Internet, the device from which that individual initiates access is assigned an IP Address. A central authority provides each Internet Service Provider a limited block of IP Addresses for use by that Internet Service Provider's customers or subscribers. The IP address can be used to locate the physical location of the computer or network that is assigned that IP address.

identifiers³ ("IDFAs") associated with Apple iPhone devices that were used by Scheme members to access App-1 in order to log into drivers' Company-1 accounts without authorization.

Overview of the Company-2 Scheme

13. Based on my conversations with representatives from a Company-2, as well as my review of documents provided by Company-2, I have learned that the fraudulent scheme typically operates as follows with respect to Company-2:

a. When an individual orders a ride through Company-2's mobile application ("App-2"), Company-2 provides the individual with information about the driver, including the driver's name, picture, and an anonymized phone number so that the rider can communicate with the driver.

b. The Scheme involves a Scheme member ordering a ride through App-2 and then cancelling the ride once he or she receives the driver's anonymized phone number.

c. After obtaining the telephone number of the driver, a Scheme member calls the driver and impersonates a representative from Company-2's customer service department. During the course of the telephone conversations with the driver, the Scheme member tells the driver that Company-2 will send the driver a link to a website the driver must use to verify the driver's information in order to obtain a bonus from Company-2.

d. The Scheme member then sends the driver a text message containing a link to a malicious website (the "Fraudulent Company-2 Website"), that is controlled by members of the Scheme. The Fraudulent Company-2 Website is designed to appear like a Company-2 website. It requests, among other information, the login credentials for the driver, including the driver's phone number, email address, and unique Company-2 password.

³ In particular, App-1 captures the Apple "identifier for advertisers" ("IDFA") identifier associated with a device when that device is used to access App-1. I have learned that an "IDFA" identifier is an advertising identification number that uniquely identifies Apple iPhone devices that have Apple's iOS 6 operating system or any later versions, and that the IDFA unique identifier is utilized to facilitate targeted advertising.

e. Scheme members use the login credential information obtained through the Fraudulent Company-2 Website to log into the driver's account through App-2 or the Company-2 web interface without the driver's authorization. Once the Scheme member has logged into the driver's Company-2 account, the Scheme member then proceeds to change the bank account information associated with the account to a bank account that either they or another Scheme member control.

f. As a result of the above-described scheme, funds that the driver earned from Company-2 are diverted instead to a Scheme member's bank account. Company-2 has informed me that Company-2 generally only sends payment to drivers' designated bank accounts on approximately a weekly basis such that it could take a number of days before a driver would realize that the bank account information associated with the driver's Company-2 account had been changed, without the driver's authorization.

Use of the Diverted Funds by Scheme Members

14. Based on the information provided by Company-1 and Company-2 in connection with this investigation, I have learned that during the course of this Scheme, thousands of Company-1 and Company-2 driver accounts were compromised as a result of the Scheme, and millions of dollars were diverted from Company-1 and Company-2 driver accounts as a result of the Scheme.

15. From reviewing bank records, I have learned that shortly after receiving unauthorized payments from Company-1 and Company-2, the Scheme members withdraw the fraudulent proceeds from the bank accounts, typically through cash withdrawals or large purchases.

Roles of the Defendants in the Scheme

16. Based on my review of materials obtained in the course of this investigation, I have identified dozens of Scheme members, including the defendants, who conspired to defraud Company-1 and Company-2, as well as their drivers, through the Scheme. These Scheme members played different roles: (i) "Recruiters," who used social media, including Snapchat, to bring new people into the Scheme and coordinate the Scheme; (ii) "Callers," who made calls to drivers impersonating Company-1 and Company-2 representatives using either their personal phones or Pinger phone numbers, as explained below, see ¶ 21(b), infra; (iii) "Account Hackers," who logged into Company-1 and Company-2 accounts to change bank account information; and (iv) "Money Receivers," who received unauthorized transfers into their bank

accounts from Company-1 and Company-2 as a result of the Scheme. Many of the Scheme members appear to have played multiple roles during the course of the Scheme. As set forth in greater detail below, the defendants appear to have played the following roles in the Scheme:

a. The following defendants appear to have acted as Recruiters: LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, and DEVON WILLIAMS, the defendants.

b. The following defendants appear to have acted as Callers: LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, DEVON WILLIAMS, and HAKEEM BALDEO, the defendants.

c. The following defendants appear to have acted as Account Hackers: LOUIS PINA, AKEEM KRUBALLY, DEVON WILLIAMS, and JOHNNY SERRANO, the defendants.

d. The following defendants appear to have acted as Money Receivers: LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, AKEEM KRUBALLY, THERESA OUTERBRIDGE, HAKEEM BALDEO, QUINTEEN LYNCH, KHALID NAZZAL, FRANCISCO VIRUET, and JOHNNY SERRANO, the defendants.

17. As set forth in more detail below, the Scheme members, including the defendants, used common phone numbers, IPs, and devices with unique IDFAs to carry out the Scheme.

LOUIS PINA's Participation in the Scheme

18. As set forth in detail below, the investigation has developed evidence indicating that LOUIS PINA, the defendant, participated in the Scheme as a Recruiter, Caller, Account Hacker, and Money Receiver. Evidence of PINA's involvement in the Scheme includes, among other things, the following: (i) unauthorized transfers from Company-1 into a bank account held in PINA's name; (ii) social media communications in which PINA discusses the Scheme; (iii) calls to drivers in connection with the Scheme from phone numbers associated with PINA; (iv) IP addresses registered to PINA that were used in furtherance of the Scheme; and (v) devices connected to PINA that were involved in making unauthorized transfers sent to PINA and other Scheme members.

19. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that LOUIS PINA, the defendant, received unauthorized transfers from Company-1, as follows:

a. Between on or about October 21, 2016 and on or about October 25, 2016, at least 21 unauthorized transfers were deposited from Company-1 into a People's Bank account held in LOUIS PINA's name ("People's Bank Account-1"). These unauthorized transfers totaled approximately \$5,652.61.

b. A review of People's Bank Account-1 shows that there were large cash withdrawals and purchases made shortly after unauthorized transfers were deposited into People's Bank Account-1. For example, between on or about October 24, 2016 and on or about October 25, 2016, Company-1 made approximately 18 unauthorized deposits into People's Bank Account-1, totaling approximately \$4,961.94. On or about October 25, 2016, approximately \$1,300 was withdrawn from People's Bank Account-1 through ATMs. Additionally, approximately \$2,400 was spent on money orders and approximately \$990 was spent at a retail store in the Bronx.

20. On or about April 5, 2017, WCDAO obtained a search warrant (the "WCDAO Search Warrant") to search the Snapchat accounts of certain individuals. I have reviewed the WCDAO Search Warrant returns as part of this investigation. Based on my review of the WCDAO Search Warrant returns, as well as my review of materials obtained in the course of this investigation, I have learned, among other things, that PINA recruited and directed Scheme members using Snapchat, as follows:

a. One of the Snapchat accounts searched as part of the WCDAO Search Warrant returns appears to belong to LOUIS PINA, the defendant (the "PINA Snapchat Account"). The photographs in the PINA Snapchat Account appear to depict PINA, based on my review of photographs of PINA contained in law enforcement databases.

b. The phone number registered to the PINA Snapchat account was also identified by PINA as his phone number in a Snapchat message sent on or about February 19, 2017 (the "PINA Phone Number").

c. The PINA Snapchat Account contains a video in which an individual is seen using a cellphone to transfer approximately \$2,192.54 from a Company-1 account to a debit card ("Debit Card-1"). The face of the individual is not visible in the video.

d. Company-1 records show that, on or about November 15, 2016, an unauthorized transfer of approximately \$2,192.54

was deposited into the bank account associated with Debit Card-1. Overall, the holder of Debit Card-1 has received approximately \$5,864.71 in unauthorized transfers from Company-1.

e. On or about January 10, 2017, PINA sent MALIK GRAY, the defendant, a Snapchat message containing a photograph of a TD Bank Debit Card ("Debit Card-2") in the name of FRANCISCO VIRUET, the defendant. On or about the same day, the bank account associated with Debit Card-2 received two unauthorized transfers from Company-1, totaling approximately \$753.13.

21. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that phone numbers associated with LOUIS PINA, the defendant, were used to call drivers as part of the Scheme, as follows:

a. A review of records provided by Company-1 shows that the PINA Phone Number was used to call 13 drivers whose Company-1 accounts were accessed without authorization during the course of the Scheme, resulting in unauthorized transfers totaling approximately \$9,570.28, of which \$4,523.35 was deposited into the bank account of a co-conspirator not named herein ("CC-1").

b. Company-1 identified two phone numbers that were used to call Company-1 drivers shortly before the unauthorized transfers were made into People's Bank Account-1. I have determined that these phone numbers are both serviced by Pinger, a free service that lets users "spoof," or mask, the number they use to make phone calls call.

c. Based on my review of materials provided by Pinger, I have learned that one of these numbers ("Pinger Phone Number-1") was used to mask the PINA Phone Number.

22. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that an IP address registered to PINA was used to log into driver accounts without authorization, as follows:

a. Between on or about October 21, 2016 and on or about February 7, 2017, a specific IP address ("IP-1") was used to log into Company-1 driver accounts, resulting in 127 unauthorized transfers from Company-1 to Scheme members totaling approximately \$32,089.27. These unauthorized transfers were deposited into People's Bank Account-1, as well as a bank

account registered to CC-1, among others. According to subscriber records obtained for the service provider for IP-1, the listed subscriber name is "Luis Pilna." The subscriber address for IP-1 is in the Bronx and matches the address for PINA.

b. According to Snapchat records, IP-1 was also used to log into and out of the PINA Snapchat Account on approximately 28 occasions between July 2016 and January 2017.

23. Based on my review of materials provided by Company-1 and my conversation with representatives from Company-1, I have learned, among other things, that devices associated with unauthorized transfers to LOUIS PINA, the defendant, were also associated with unauthorized transfers to other Scheme members, as follows:

a. Company-1 was able to identify five devices with unique IDFAs associated with the unauthorized transfers into People's Bank Account-1.

b. One of those five IDFAs ("IDFA-1") was linked to approximately 69 unauthorized transfers totaling \$31,716.86. These unauthorized transfers were sent to People's Bank Account-1, and, as set forth below, see ¶¶ 62 and 71(a), infra, accounts registered to QUINTEEN LYNCH and FRANCISCO VIRUET, the defendants, as well as CC-1 and another co-conspirator not named herein ("CC-2"), among others.

c. A second of those five IDFAs ("IDFA-2") was linked to approximately 26 unauthorized transfers approximately totaling \$6,621.89. These unauthorized transfers were sent to People's Bank Account-1 and an account registered to CC-1.

24. Based on my conversation with a Company-1 driver ("Driver-1"), as well as my review of Company-1 records relating to Driver-1, I have learned that Driver-1 was a victim of the Scheme, as follows:

a. On or about October 23, 2016, Driver-1 received a call from Pinger Phone Number-1. Driver-1 stated that the caller said, in sum and substance, that he was calling from Company-1 to verify Driver-1's information, and then asked for the unique code Company-1 had just sent to Driver-1. Driver-1 then gave the caller the code.

b. On or about October 23, 2016 and October 24, 2016, approximately two unauthorized transfers were sent from Driver-1's Company-1 account to People's Bank Account-1. These transfers totaled approximately \$795.17.

25. Based on my discussions with representatives of Company-1 and Company-2, I have learned that LOUIS PINA, the defendant, has never been employed as a driver by Company-1 or Company-2.

MALIK GRAY's Participation in the Scheme

26. As set forth in detail below, the investigation has developed evidence indicating that MALIK GRAY, the defendant, participated in the Scheme as a Recruiter, Caller, and Money Receiver. Evidence of GRAY's involvement in the Scheme includes the following: (i) unauthorized transfers from Company-1 into a bank account held in GRAY's name; (ii) social media communications in which GRAY discusses the Scheme; (iii) calls to drivers from phone numbers associated with GRAY; and (iv) devices linked to GRAY that are associated with unauthorized transfers sent to GRAY and other Scheme members.

27. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that MALIK GRAY, the defendant, received unauthorized transfers from Company-1, as follows:

a. Between on or about October 27, 2016 and on or about January 23, 2017, at least approximately 93 unauthorized transfers were deposited from Company-1 into a TD Bank account held GRAY's name ("TD Bank Account-1"). These unauthorized transfers totaled approximately \$25,885.03.

b. A review of TD Bank Account-1 shows large withdrawals and purchases shortly after unauthorized transfers from Company-1 were deposited into TD Bank Account-1. For example, on or about January 18, 2017, Company-1 made an unauthorized transfer into TD Bank Account-1 totaling approximately \$2,239.29. On or about the same day, approximately \$2,420 was withdrawn from TD Bank Account-1 through an ATM located at a TD bank branch in Manhattan, New York.

28. Based on my review of the WCDAO Search Warrant returns, as well as my review of materials obtained in the course of this investigation, I have learned, among other

things, that MALIK GRAY, the defendant, recruited and directed Scheme members using Snapchat, as follows:

a. One of the Snapchat accounts searched as part of the WCDAO Search Warrant returns appears to belong to MALIK GRAY, the defendant (the "GRAY Snapchat Account"). The photographs in the GRAY Snapchat Account appear to depict GRAY, based on my review of photographs of GRAY contained in law enforcement databases.

b. On or about May 31, 2016, GRAY sent a Snapchat message to a Scheme member, which stated: "Lemme use ur number for a [Company-1]."

c. On or about November 6, 2016, GRAY sent a Snapchat message to a Scheme member, which stated: "U cud get me a number for [Company-1] plz bro."

d. As stated herein, see ¶ 20(e), supra, on or about January 10, 2017, GRAY received a Snapchat message from LOUIS PINA, the defendant, with a photograph of Debit Card-2, which subsequently led to two unauthorized transfers from Company-1.

29. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that phone numbers associated with MALIK GRAY, the defendant, were used to call drivers as part of the Scheme, as follows:

a. Company-1 identified five Pinger phone numbers used to call Company-1 drivers shortly before the unauthorized transfers into TD Bank Account-1. In addition, these numbers were used to call Company-1 drivers on multiple other occasions, leading to unauthorized transfers to Scheme members, including GEORGE JOSEPH, the defendant, totaling approximately \$39,647.87.

b. According to subscriber records obtained from Pinger, approximately three of the above-referenced phone numbers were registered to a phone number that, based on my review of telephone provider records, was subscribed to by GRAY (the "GRAY Phone Number").

c. Two of above-referenced Pinger phone numbers were registered to a different phone number that, based on my review of telephone provider records, was also subscribed to by GRAY. However, based on my review of the WCDAO Search Warrant returns, it appears that this number is actually used by co-conspirator GEORGE JOSEPH, the defendant ("JOSEPH Phone Number-1"), as

JOSEPH identifies it as his number in multiple Snapchat messages.

30. Based on my review of materials provided by Company-1 and my conversation with representatives from Company-1, I have learned, among other things, that devices associated with unauthorized transfers to MALIK GRAY, the defendant, were also associated with unauthorized transfers to other Scheme members, as follows:

a. Company-1 was able to identify three devices with unique IDFAs associated with the unauthorized transfers into TD Bank Account-1, which, as discussed above, was held in GRAY's name.

b. One of those three IDFAs ("IDFA-3") was linked to approximately 16 additional unauthorized transfers totaling approximately \$3,110.59, of which approximately \$676.86 was deposited into a TD Bank Account held in JOSEPH's name ("TD Bank Account-2").

c. Another of those three IDFAs ("IDFA-4") was linked to approximately 24 additional unauthorized transfers totaling approximately \$3,740.28, of which approximately \$3,561.63 was deposited into TD Bank Account-2.

31. Based on my conversation with a Company-1 driver ("Driver-2"), as well as my review of Company-1 records relating to Driver-2, I have learned that Driver-2 was a victim of the Scheme, as follows:

a. On or about October 31, 2016, Driver-2 received a call from a Pinger phone number registered to the GRAY Phone Number ("Pinger Phone Number-2"). Driver-2 stated that the caller said, in sum and substance, that he was calling from Company-1's fraud team and that Driver-2's account had been hacked, but that the caller would send a code to verify Driver-2's information. After Driver-2 received a text message containing the code, Driver-2 provided it to the caller.

b. On or about October 31, 2016, approximately four unauthorized transfers were sent to TD Bank Account-1 from Driver-2's Company-1 account. These transfers totaled approximately \$311.63.

32. Based on my discussions with representatives of Company-1 and Company-2, I have learned that MALIK GRAY, the

defendant, has never been employed as a driver by Company-1 or Company-2.

GEORGE JOSEPH's Participation in the Scheme

33. As set forth in detail below, the investigation has developed evidence indicating that GEORGE JOSEPH, the defendant, participated in the Scheme as a Recruiter, Caller, and Money Receiver. Evidence of JOSEPH's involvement in the Scheme includes the following: (i) unauthorized transfers from Company-1 into bank accounts held in JOSEPH's name; (ii) social media communications in which JOSEPH discusses the Scheme; (iii) calls to Company-1 and Company-2 drivers from phone numbers associated with JOSEPH; and (iv) devices linked to unauthorized transfers sent to JOSEPH and other Scheme members.

34. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that GEORGE JOSEPH, the defendant, received unauthorized transfers from Company-1, as follows:

a. Between on or about October 25, 2016 and on or about January 23, 2017, at least approximately 85 unauthorized transfers from Company-1 were deposited into TD Bank Account-2, which, as stated herein, was held in JOSEPH's name. See ¶ 30(b), supra. These unauthorized transfers totaled approximately \$19,616.49.

b. A review of TD Bank Account-2 shows large withdrawals and purchases shortly after unauthorized transfers from Company-1 were deposited into TD Bank Account-2. For example, on or about October 31, 2016, Company-1 made approximately 20 unauthorized transfers into TD Bank Account-2 totaling approximately \$5,883.89. On or about the same day, approximately \$1,904 was withdrawn from TD Bank Account-2 through ATMs located in Pelham, Mt. Vernon, Yonkers, and the Bronx, New York. Additionally, approximately \$3,472.37 was spent using TD Bank Account-2 at various stores in White Plains, Yonkers, the Bronx, and Woodbury, New York.

35. Based on my review of the WCD AO Search Warrant returns, as well as my review of materials obtained in the course of this investigation, I have learned, among other things, that GEORGE JOSEPH, the defendant, recruited and directed Scheme members using Snapchat, as follows:

a. One of the Snapchat accounts searched as part of the WCD AO Search Warrant returns appears to belong to GEORGE

JOSEPH, the defendant (the "JOSEPH Snapchat Account"). The photographs in the JOSEPH Snapchat Account appear to depict JOSEPH, based on my review of photographs of JOSEPH contained in law enforcement databases.

b. On or about December 5, 2016, JOSEPH engaged in the following conversation over Snapchat with an account that, as stated herein, see ¶ 42(a), infra, I believe belongs to AKEEM KRUBALLY, the defendant (the "KRUBALLY Snapchat Account"):

KRUBALLY: This is my shit [Debit Card-3]

c. On or about December 12, 2016, Debit Card-3 was added to the Company-1 account of a Company-1 driver. On or about the same date, an unauthorized transfer of approximately \$1,283.16 went to a TD Bank account ("TD Bank Account-3") associated with Debit Card-3. Based on my review of documents obtained in the course of this investigation, TD Bank Account-3 is held in the name of AKEEM KRUBALLY, the defendant.

d. On or about December 4, 2016 and December 5, 2016, JOSEPH sent two Snapchat messages containing screenshots of Company-1 deposit confirmations from App-1. These screenshots correspond to unauthorized transfers from Company-1 to Scheme members.

36. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that phone numbers associated with GEORGE JOSEPH, the defendant, were used to call drivers as part of the Scheme, as follows:

a. Company-1 identified at least eight Pinger phone numbers that were used to call Company-1 drivers shortly before the unauthorized transfers to TD Bank Account-2. According to subscriber records obtained from Pinger, four of the Pinger phone numbers were registered to JOSEPH Phone Number-1.

b. Additionally, JOSEPH Phone Number-1 made calls to Company-1 drivers that led to three unauthorized transfers to TD Bank Account-2, totaling approximately \$174.46.

c. Based on my review of the WCDAO Search Warrant returns, it appears that JOSEPH uses a second phone ("JOSEPH Phone Number-2") that he identified in messages sent using the JOSEPH Snapchat Account.

d. On or about January 29, 2017, JOSEPH Phone Number-2 sent text messages to Company-2 drivers on

approximately six occasions, directing Company-2 drivers to input their log-in credentials into the Fraudulent Company-2 Website. The resulting unauthorized transfers totaled approximately \$2,909.39.

37. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that an IP address registered to GEORGE JOSEPH, the defendant, was used to log into driver accounts without authorization, as follows:

a. Between on or about October 23, 2016 and on or about November 3, 2016, a specific IP address ("IP-2") was used to log into Company-1 driver accounts, resulting in approximately 44 unauthorized transfers from Company-1 to Scheme members totaling approximately \$6,845.47. These unauthorized transfers were deposited into TD Bank Account-1 and TD Bank Account-2, among other accounts. According to subscriber information obtained from the service provider for IP-2, the listed subscriber for IP-2 is GEORGE JOSEPH, the defendant.

38. Based on my review of materials provided by Company-1 and my conversation with representatives from Company-1, I have learned, among other things, that devices associated with unauthorized transfers to GEORGE JOSEPH, the defendant, were also associated with unauthorized transfers to other Scheme members. Specifically, Company-1 was able to identify six devices with unique IDFAs associated with the unauthorized transfers into TD Bank Account-2, which as discussed above, was held in JOSEPH's name. These IDFAs were linked to an approximately 103 additional unauthorized transfers, totaling approximately \$33,897.87, from Company-1 to MALIK GRAY, FRANCISCO VIRUET, and THERESA OUTERBRIDGE, the defendants, among others.

39. Based on my discussions with representatives of Company-1 and Company-2, I have learned that GEORGE JOSEPH, the defendant, has never been employed as a driver by Company-1 or Company-2.

AKEEM KRUBALLY's Participation in the Scheme

40. As set forth in detail below, the investigation has developed evidence indicating that AKEEM KRUBALLY, the defendant, participated in the Scheme as a Recruiter, Account Hacker, and Money Receiver. Evidence of KRUBALLY's involvement in the Scheme includes the following: (i) unauthorized transfers from Company-1 and Company-2 into a bank account held in

KRUBALLY's name; (ii) social media communications in which KRUBALLY discusses the Scheme; and (iii) a device linked to KRUBALLY that was also linked to unauthorized transfers sent to KRUBALLY and other Scheme members.

41. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that AKEEM KRUBALLY, the defendant, received unauthorized transfers from Company-1 and Company-2, as follows:

a. Between on or about October 27, 2016 and on or about June 14, 2017, at least approximately 69 unauthorized transfers from Company-2 were deposited into TD Bank Account-3, which, as stated herein, was held in KRUBALLY's name. See ¶ 35(c), supra. These unauthorized transfers totaled approximately \$31,683.49.

b. Between on or about October 27, 2016 and on or about December 12, 2016, at least approximately seven unauthorized transfers from Company-1 were deposited into TD Bank Account-3. These unauthorized transfers totaled approximately \$1,760.46.

c. A review of TD Bank Account-3 shows large withdrawals shortly after unauthorized transfers from Company-1 and Company-2 were deposited into TD Bank Account-3. For example, on or about March 15, 2017, Company-2 made an unauthorized transfer of \$2,535.25 into TD Bank Account-3. On or about the same day, \$2,100 was withdrawn from TD Bank Account-3.

42. Based on my review of the WCDAO Search Warrant returns, as well as my review of materials obtained in the course of this investigation, I have learned, among other things, that AKEEM KRUBALLY, the defendant, recruited and directed Scheme members using Snapchat, as follows:

a. One of the Snapchat accounts searched as part of the WCDAO Search Warrant returns appears to belong to KRUBALLY (the "KRUBALLY Snapchat Account"). The photographs in the KRUBALLY Snapchat Account appear to depict KRUBALLY, based on my review of photographs of KRUBALLY contained in law enforcement databases.

b. As stated herein, see ¶¶ 35(b)-(c), supra, on or about December 5, 2016, KRUBALLY engaged in a Snapchat conversation with GEORGE JOSEPH, the defendant, regarding Debit Card-3, which was used in connection with an unauthorized transfer to TD Bank Account-3.

c. On or about January 30, 2017, KRUBALLY engaged in the following Snapchat conversation with an account that I believe belongs to a co-conspirator not named herein ("CC-3"):

KRUBALLY: Just need that chase shit
KRUBALLY: I do [Company-1] to
KRUBALLY: Copy
CC-3: Say that so boom Im a drop this one and some [Company-1] shit on both and Im a break bread with you off everything.

43. Based on my review of materials provided by Company-1 and my conversation with representatives from Company-1, I have learned, among other things, that a device associated with AKEEM KRUBALLY, the defendant, was used to log into driver accounts without authorization, as follows:

a. A Company-1 passenger account that appears to be connected to KRUBALLY was created on or about October 28, 2016 (the "KRUBALLY Company-1 Account"). Subscriber information for the KRUBALLY Company-1 Account indicates that the account was registered to a particular email address (the "KRUBALLY Email") and phone number (the "KRUBALLY Phone Number"). The KRUBALLY Email and KRUBALLY Phone Number were both listed in the account opening documents for TD Bank Account-3, which is held in KRUBALLY's name.

b. The device with an IDFA associated with the creation of the KRUBALLY Company-1 Account ("IDFA-5") is associated with approximately 40 unauthorized transfers from Company-1, totaling approximately \$11,875.01, including approximately \$396.79 that was transferred to KRUBALLY.

44. Based on my discussions with representatives of Company-1 and Company-2, I have learned that AKEEM KRUBALLY, the defendant, has never been employed as a driver by Company-1 or Company-2.

THERESA OUTERBRIDGE's Participation in the Scheme

45. As set forth in detail below, the investigation has developed evidence indicating that THERESA OUTERBRIDGE, the defendant, participated in the Scheme as a Money Receiver. Evidence of OUTERBRIDGE's involvement in the Scheme includes the following: (i) unauthorized transfers from Company-1 into bank accounts held in OUTERBRIDGE's name; and (ii) devices linked to unauthorized transfers sent to OUTERBRIDGE and other Scheme members.

46. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that THERESA OUTERBRIDGE, the defendant, received unauthorized transfers from Company-1, as follows:

a. Between on or about October 31, 2016 and on or about January 20, 2017, at least approximately 43 unauthorized transfers from Company-1 were deposited into a Citibank account held in OUTERBRIDGE's name ("Citibank Account-1") and a Keybank account held in OUTERBRIDGE's name ("Keybank Account-1"). These unauthorized transfers totaled approximately \$9,098.09.

b. A review of Citibank Account-1 shows large withdrawals and purchases shortly after unauthorized transfers from Company-1 were deposited into Citibank Account-1. For example, on or about November 14, 2016, Company-1 made unauthorized transfers into Citibank Account-1 totaling approximately \$2,129.10. On or about the same date, approximately \$1,360 was withdrawn from Citibank Account-1. Additionally, approximately \$246.68 was spent at a store in White Plains, New York.

47. Based on my review of materials provided by Company-1 and my conversation with representatives from Company-1, I have learned, among other things, that devices associated with unauthorized transfers to THERESA OUTERBRIDGE, the defendant, were also associated with unauthorized transfers to other Scheme members, as follows:

a. Company-1 was able to identify two devices with unique IDFAs associated with the unauthorized transfers into Citibank Account-1 and Keybank Account-1.

b. As stated herein, see ¶ 38, supra, one of the two IDFAs ("IDFA-6") was linked to approximately 55 unauthorized transfers from Company-1 totaling over \$11,000 that were sent to OUTERBRIDGE and GEORGE JOSEPH, the defendant, and others.

c. The other IDFA ("IDFA-7") was linked to approximately 54 unauthorized transfers from Company-1 totaling over \$27,000 that were sent to OUTERBRIDGE, FRANCISCO VIRUET, and others.

48. Based on my conversation with a Company-1 driver ("Driver-3"), as well as my review of Company-1 records relating to Driver-3, I have learned that Driver-3 was a victim of the Scheme, as follows:

a. On or about November 1, 2016, Driver-3 received a call from an individual who stated, in sum and substance, that he was a Company-1 representative and that Driver-3's Company-1 account had been flagged for fraudulent activity. The caller told Driver-3 that Driver-3 had to verify Driver-3's identity by providing Driver-3's name and the unique code Company-1 sent Driver-3. Driver-3 provided the requested information.

b. On or about the same date, Citibank Account-1 received over approximately \$1,500 in unauthorized transfers from Driver-3's Company-1 account.

49. Based on my discussions with representatives of Company-1 and Company-2, I have learned that THERESA OUTERBRIDGE, the defendant, has never been employed as a driver by Company-1 or Company-2.

DEVON WILLIAMS's Participation in the Scheme

50. As set forth in detail below, the investigation has developed evidence indicating that DEVON WILLIAMS, the defendant, participated in the Scheme as a Recruiter and Account Hacker. Evidence of WILLIAMS's involvement in the Scheme includes the following: (i) social media communications in which WILLIAMS discusses the Scheme; and (ii) a device linked to WILLIAMS that was also linked with unauthorized transfers to other Scheme members.

51. Based on my review of the WCDAO Search Warrant returns, as well as my review of materials obtained in the course of this investigation, I have learned, among other things, that DEVON WILLIAMS, the defendant, recruited and directed Scheme members using Snapchat, as follows:

a. One of the Snapchat accounts searched as part of the WCDAO Search Warrant returns appears to belong to WILLIAMS (the "WILLIAMS Snapchat Account"). The photographs in the WILLIAMS Snapchat Account appear to depict WILLIAMS, based on my review of photographs of WILLIAMS contained in law enforcement databases.

b. On or about April 5, 2017, WILLIAMS engaged in the following conversation over Snapchat with an account that I believe belongs CC-2:

WILLIAMS: I could use ya TD today
CC-2: I need My Card That's Where All My Money Is

WILLIAMS: Send the card

c. CC-2 then sent WILLIAMS a Snapchat message containing a photograph of a TD Bank Debit Card in CC-2's name ("Debit Card-4"). On or about April 10, 2017, there were two unauthorized transfers from Company-2 to Debit Card-2 totaling approximately \$1,024.11.

52. Based on my review of materials provided by Company-1 and my conversation with representatives from Company-1, I have learned, among other things, that a device associated with DEVON WILLIAMS, the defendant, was used to log into driver accounts without authorization, as follows:

a. A Company-1 passenger account that appears to be connected to WILLIAMS was created using on or about December 1, 2016 (the "WILLIAMS Company-1 Account"). The WILLIAMS Company-1 Account listed a particular phone number (the "WILLIAMS Phone Number") as the registered subscriber phone number. In addition, WILLIAMS sent Snapchat messages using the WILLIAMS Snapchat Account in which he identified the WILLIAMS Phone Number as his own.

b. A device with an IDFA associated with the WILLIAMS Company-1 Account ("IDFA-8") is associated with approximately 52 unauthorized transfers from Company-1, totaling approximately \$10,854.84, including unauthorized transfers to QUINTEEN LYNCH, the defendant, among others.

53. Based on my discussions with representatives of Company-1 and Company-2, I have learned that DEVON WILLIAMS, the defendant, has never been employed as a driver by Company-1 or Company-2.

HAKHEEM BALDEO's Participation in the Scheme

54. As set forth in detail below, the investigation has developed evidence indicating that HAKHEEM BALDEO, the defendant, participated in the Scheme as a Caller and Money Receiver. Evidence of BALDEO's involvement in the Scheme includes the following: (i) unauthorized transfers from Company-1 into bank accounts held in BALDEO's name; and (ii) calls to drivers from phone numbers associated with BALDEO.

55. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that HAKHEEM BALDEO, the defendant, received unauthorized transfers from Company-1 and Company-2, as follows:

a. Between on or about November 8, 2016 and on or about January 23, 2017, at least approximately 21 unauthorized transfers from Company-1 were deposited into a Citibank account ("Citibank Account-2") and a Keybank account ("Keybank Account-2"), both held in BALDEO's name. These unauthorized transfers totaled approximately \$7,649.17. During approximately the same time period, Company-2 deposited at least approximately \$9,749.99 into Keybank Account-2.

b. A review of Citibank Account-2 shows large withdrawals and purchases shortly after unauthorized transfers from Company-1 were deposited into Citibank Account-2. For example, on or about November 8, 2016, Company-1 made unauthorized transfers into Citibank Account-2 totaling approximately \$5,493.52. Between on or about November 8, 2016 and on or about November 15, 2016, approximately \$2,960 was withdrawn from Citibank Account-2. Additionally, approximately \$951.53 was spent using Citibank Account-2 through an online retailer.

56. Based on my review of records obtained in the course of this investigation, I have learned, among other things, a phone number associated with HAKEEM BALDEO, the defendant, was used to call drivers as part of the Scheme, as follows:

a. Company-1 identified approximately 20 unauthorized transfers to Citibank Account-2 associated with a particular Pinger phone number ("Pinger Phone Number-3"). According to subscriber records obtained from Pinger, Pinger Phone Number-3 was registered to a phone number that, based on my review of law enforcement databases, belongs to BALDEO (the "BALDEO Phone Number"). According to records provided by Company-1, Pinger Phone Number-3 was used to call Company-1 drivers shortly before approximately 22 additional unauthorized transfers from Company-1 to Scheme members, totaling approximately \$5,378.39.

57. Based on my conversation with a Company-1 driver ("Driver-4"), as well as my review of Company-1 records relating to Driver-4, I have learned that Driver-4 was a victim of the Scheme, as follows:

a. On or about November 8, 2016, Driver-4 received a call from Pinger Phone Number-3, which, as discussed above, I believe was used by HAKEEM BALDEO, the defendant. Driver-4 stated that the caller said, in sum and substance, that he was a customer service manager from Company-1, and that the caller would send a four-digit code to Driver-4 to verify Driver-4's

identity. When Driver-4 received the code, Driver-4 shared it with the caller.

b. On or about the same date, two unauthorized transfers were sent to Citibank Account-2 from Driver-4's Company-1 account. These transfers totaled approximately \$1,297.05.

58. Based on my discussions with representatives of Company-1 and Company-2, I have learned that HAKEEM BALDEO, the defendant, has never been employed as a driver by Company-1 or Company-2.

QUINTEEN LYNCH's Participation in the Scheme

59. As set forth in detail below, the investigation has developed evidence indicating that QUINTEEN LYNCH, the defendant, participated in the Scheme as a Money Receiver. Evidence of LYNCH's involvement in the Scheme includes the following: (i) unauthorized transfers from Company-1 and Company-2 into a bank account held in LYNCH's name; (ii) calls to drivers from phone numbers associated with unauthorized transfers sent to LYNCH and other Scheme members; (iii) calls with other Scheme members around the time of unauthorized transfers; and (iv) devices linked to unauthorized transfers sent to LYNCH and other Scheme members.

60. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that QUINTEEN LYNCH, the defendant, received unauthorized transfers from Company-1 and Company-2, as follows:

a. Between on or about December 2, 2016 and on or about January 28, 2017, at least approximately 33 unauthorized transfers were deposited from Company-1 into a TD Bank account held in LYNCH's name ("TD Bank Account-4"). These unauthorized transfers totaled approximately \$12,158.89. Between on or about February 17, 2017 and on or about June 9, 2017, at least approximately 68 unauthorized transfers were deposited by Company-2 into TD Bank Account-4, totaling approximately \$27,737.96. These unauthorized transfers were the only source of income during this period in TD Bank Account-4.

b. A review of TD Bank Account-4 shows large withdrawals and purchases shortly after unauthorized transfers from Company-1 and Company-2 were deposited into TD Bank Account-4. For example, on or about April 10, 2017, Company-2 made unauthorized transfers into TD Bank Account-4 totaling

approximately \$3,318.05. On or about the same day, \$3,260 was withdrawn from TD Bank Account-4.

61. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that phone numbers associated with unauthorized transfers to QUINTEEN LYNCH, the defendant, were also associated with unauthorized transfers to other Scheme members, as follows:

a. Company-1 identified a Pinger phone number ("Pinger Phone Number-4") that was used to call Company-1 drivers shortly before two unauthorized transfers from Company-1 into TD Bank Account-4, which as described above, is held in LYNCH's name. Pinger Phone Number-4 was also used to call a Company-1 driver on another occasion, leading to an unauthorized transfer into the account of a CC-2.

b. Company-1 identified a second Pinger phone number ("Pinger Phone Number-5") that was used to call Company-1 drivers shortly before three unauthorized transfers from Company-1 into TD Bank Account-4. According to subscriber records obtained from Pinger, Pinger Phone Number-5 was registered to the WILLIAMS Phone Number.

c. The account opening documents for TD Bank Account-4 list a phone number that I believe is associated with LYNCH (the "LYNCH Phone Number"). On or about January 16, 2017, the LYNCH Phone Number sent four text messages to the PINA Phone Number and received or placed eleven phone calls with the PINA Phone Number. Shortly thereafter, the LYNCH Phone Number called the WILLIAMS Phone Number eight times.

d. At approximately 7:00 p.m. on or about January 16, 2017, Pinger Phone Number-5, which was registered to the WILLIAMS Phone Number, placed a call to a Company-1 driver. On or about the following day, TD Bank Account-4 received an unauthorized transfer from Company-1 totaling approximately \$7,570.59.

62. Based on my review of materials provided by Company-1 and my conversation with representatives from Company-1, I have learned, among other things, that a device associated with unauthorized transfers to QUINTEEN LYNCH, the defendant, was also associated with unauthorized transfers to other Scheme members. Specifically, as discussed in detail above in paragraph 23(b), supra, a device associated with IDFA-1 was associated with two unauthorized transfers into TD Bank Account-4, which was held in LYNCH's name, and also associated with

other unauthorized transfers to accounts associated with LOUIS PINA and FRANCISCO VIRUET, the defendants.

63. Based on my conversation with a Company-2 driver ("Driver-5"), as well as my review of Company-2 records relating to Driver-5, I have learned that Driver-5 was a victim of the Scheme, as follows:

a. On or about March 5, 2017, Driver-5 received a call from an individual who told Driver-5, in sum and substance, that Driver-5 had won \$200 and that the caller would send a link to Driver-5's cellphone where Driver-5 could input Driver-5's Company-2 username and password to claim Driver-5's prize. After receiving a text message, Driver-5 entered the log-in credentials. Driver-5 then received a notification from Company-2 that Driver-5's bank account information had been changed.

b. On or about March 6, 2017, an unauthorized transfer was sent to TD Bank Account-4 from Driver-5's Company-2 account. This transfer totaled approximately \$1,053.83.

64. Based on my discussions with representatives of Company-1 and Company-2, I have learned that QUINTEEN LYNCH, the defendant, has never been employed as a driver by Company-1 or Company-2.

KHALID NAZZAL's Participation in the Scheme

65. As set forth in detail below, the investigation has developed evidence indicating that KHALID NAZZAL, the defendant, participated in the Scheme as a Money Receiver. Evidence of NAZZAL's involvement in the Scheme includes the following: (i) unauthorized transfers from Company-1 into a bank account held in NAZZAL's name; and (ii) calls to drivers from phone numbers associated with unauthorized transfers sent to NAZZAL and other Scheme members.

66. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that KHALID NAZZAL, the defendant, received unauthorized transfers from Company-1 and Company-2, as follows:

a. Between on or about January 23, 2017 and on or about April 10, 2017, at least approximately four unauthorized transfers from Company-1 and approximately 54 unauthorized transfers from Company-2 were deposited into a TD Bank account

held in NAZZAL's name ("TD Bank Account-5"). These unauthorized transfers totaled approximately \$1,449.35 from Company-1 and approximately \$22,212.32 from Company-2. These unauthorized transfers were the only significant source of income in TD Bank Account-5 during this time period.

b. A review of TD Bank Account-5 shows large withdrawals and purchases shortly after unauthorized transfers from were deposited into TD Bank Account-5. For example, on or about March 13, 2017, Company-2 made unauthorized transfers into TD Bank Account-5 totaling approximately \$4,204.48. On or about the same date, approximately \$3,800 was withdrawn from TD Bank Account-5.

67. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that a phone number associated with unauthorized transfers to KHALID NAZZAL, the defendant, was associated with GEORGE JOSEPH, the defendant, as follows:

a. Company-1 identified two unauthorized transfers to TD Bank Account-5 associated with a particular Pinger phone number ("Pinger Phone Number-6"). According to subscriber records obtained from Pinger, Pinger Phone Number-6 was registered to JOSEPH Phone Number-1.

68. Based on my discussions with representatives of Company-1 and Company-2, I have learned that KHALID NAZZAL, the defendant, has never been employed as a driver by Company-1 or Company-2.

FRANCISCO VIRUET's Participation in the Scheme

69. As set forth in detail below, the investigation has developed evidence indicating that FRANCISCO VIRUET, the defendant, participated in the Scheme as a Money Receiver. Evidence of VIRUET's involvement in the Scheme includes the following: (i) unauthorized transfers from Company-1 into a bank account held VIRUET's name; and (ii) a device linked to unauthorized transfers sent to VIRUET and other Scheme members.

70. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that FRANCISCO VIRUET, the defendant, received unauthorized transfers from Company-1, as follows:

a. Between on or about December 7, 2016 and on or about April 10, 2017, approximately 25 unauthorized transfers

from Company-1 were deposited into a TD Bank account held in VIRUET's name ("TD Bank Account-6"). These unauthorized transfers totaled approximately \$11,301.39. These unauthorized transfers were the only source of income in TD Bank Account-6 during this time period.

b. A review of TD Bank Account-6 shows large withdrawals and purchases shortly after unauthorized transfers from were deposited into TD Bank Account-6. For example, on or about January 17, 2017, Company-1 made unauthorized transfers into TD Bank Account-6 totaling approximately \$5,160.47. On or about the same date, approximately \$4,358.27 was withdrawn from TD Bank Account-6 in 14 separate ATM transactions. Moreover, on or about the same date, three retail purchases were made using TD Bank Account-6, totaling approximately \$604.98.

71. Based on my review of materials provided by Company-1 and my conversation with representatives from Company-1, I have learned, among other things, that devices associated with unauthorized transfers to FRANCISCO VIRUET, the defendant, were also associated with unauthorized transfers to other Scheme members, as follows:

a. As stated herein, see ¶ 23(b), supra, IDFA-1 was associated with unauthorized transfers into TD Bank Account-6, held in VIRUET's name.

b. Company-1 was able to identify a unique IDFA ("IDFA-9") that was linked to approximately 56 unauthorized transfers from Company-1 totaling approximately \$16,409.58. These unauthorized transfers were sent to VIRUET and JOHNNY SERRANO, the defendant, among others. Four of these unauthorized transfers occurred shortly after telephone calls to Company-1 drivers from Pinger Phone Number-1.

72. Based on my conversation with a Company-1 driver ("Driver-6"), as well as my review of Company-1 records relating to Driver-6, I have learned that Driver-6 was a victim of the Scheme, as follows:

a. On or about February 4, 2017 Driver-6 received a call from an individual who said, in sum and substance, that he worked for Company-1. The caller said that Driver-6 was receiving a bonus from Company-1, and that the caller would send a four-digit code to Driver-6's cellphone to claim the bonus. When Driver-6 received the code, Driver-6 shared it with the caller. Driver-6 later realized that someone had accessed Driver-6's Company-1 account and changed the bank information,

resulting in unauthorized transfers from the account of approximately \$1,000.

b. On or about February 4, 2017, one unauthorized transfer was sent from Driver-6's Company-1 account to TD Bank Account-6, totaling approximately \$1,150.65. The unauthorized login to Driver-6's Company-1 account is associated with IDFA-1.

73. Based on my discussions with representatives of Company-1 and Company-2, I have learned that FRANCISCO VIRUET, the defendant, has never been employed as a driver by Company-1. VIRUET registered as a driver for Company-2 in or about January 2017, but, according to Company-2 records, has never driven since registering.

JOHNNY SERRANO's Participation in the Scheme

74. As set forth in detail below, the investigation has developed evidence indicating that JOHNNY SERRANO, the defendant, participated in the Scheme as an Account Hacker and Money Receiver. Evidence of SERRANO's involvement in the Scheme includes the following: (i) unauthorized transfers from Company-1 and Company-2 into a bank accounts held in SERRANO's name; (ii) calls to drivers from phone numbers associated with unauthorized transfers sent to SERRANO and other Scheme members; and (iii) SERRANO's use of an IP address that was also used for unauthorized logins into Company-1 accounts.

75. Based on my review of bank records obtained in the course of this investigation, I have learned, among other things, that JOHNNY SERRANO, the defendant, received unauthorized transfers from Company-1 and Company-2, as follows:

a. Between on or about October 19, 2016 and on or about March 17, 2017, at least 25 unauthorized transfers from Company-1 and 89 unauthorized transfers from Company-2 were deposited into a Popular Community Bank account held in SERRANO's name ("Popular Community Bank Account-1"). These unauthorized transfers totaled approximately \$3,982.81 for Company-1 and approximately \$33,112.24 for Company-2.

b. A review of Popular Community Bank Account-1 shows that there were large cash withdrawals and purchases made shortly after unauthorized transfers were deposited into People's Bank Account-1. For example, on or about February 21, 2017, Company-2 made unauthorized transfers into People's Bank Account-1 totaling approximately \$3,830.01. On or about the same day, about approximately \$2,000 was withdrawn from Popular

Community Bank Account-1. Additionally, approximately \$1,700 was spent at a casino in Yonkers.

76. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that phone numbers associated with unauthorized transfers to JOHNNY SERRANO, the defendant, were also associated with unauthorized transfers to other Scheme members, as follows:

a. Company-1 identified three Pinger phone numbers associated with the unauthorized transfers into Popular Community Bank Account-1.

b. One of these numbers ("Pinger Phone Number-7") was associated with approximately 55 unauthorized transfers from Company-1, including transfers to CC-1.

c. Another of these numbers ("Pinger Phone Number-8") was associated with approximately 37 unauthorized transfers from Company-1, including transfers to CC-1.

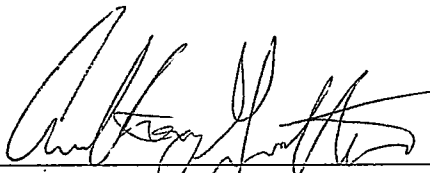
77. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that SERRANO used an IP address registered to LOUIS PINA, the defendant, on or about the same day as that IP address was used to log into driver accounts without authorization, as follows:

a. IP-1, which, as stated herein, was registered to "Luis Pilna," see ¶ 22(a), supra, was used to log into Company-1 driver accounts without authorization on or about October 26, 2016.

b. On or about the same date, IP-1 was used to log into a Snapchat account that appears to belong to SERRANO.

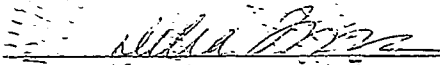
78. Based on my discussions with representatives of Company-1 and Company-2, I have learned that JOHNNY SERRANO, the defendant, has never been employed as a driver by Company-1 or Company-2.

WHEREFORE, deponent respectfully requests that warrants be issued for the arrests of LOUIS PINA, MALIK GRAY, GEORGE JOSEPH, AKEEM KRUBALLY, THERESA OUTERBRIDGE, DEVON WILLIAMS, HAKEEM BALDEO, QUINTEEN LYNCH, KHALID NAZZAL, FRANCISCO VIRUET, and JOHNNY SERRANO, the defendants, and that they be imprisoned or bailed, as the case may be.



Criminal Investigator Anthony Giattino
United States Attorney's Office
Southern District of New York

Sworn to before me this
27th day of November, 2017



THE HONORABLE DEBRA FREEMAN
UNITED STATES CHIEF MAGISTRATE JUDGE
SOUTHERN DISTRICT OF NEW YORK