

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, THALIA CAQUIAS and TANESHA FORD, 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 THALIA CAQUIAS and TANESHA FORD, 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 THALIA CAQUIAS and TANESHA FORD, 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 THALIA CAQUIAS and TANESHA FORD, 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 January 18, 2017, THALIA CAQUIAS, the defendant, received approximately \$1,360 in funds that had been obtained through unauthorized access to accounts belonging to drivers for a ride-sharing company.

b. On or about January 15, 2017, CAQUIAS received funds that had been obtained through unauthorized access to an account belonging to a ride-sharing driver, and on or about January 15, 2017 and on or about January 16, 2017, CAQUIAS withdrew funds from her bank accounts at an ATM located in the Bronx, New York.

c. On or about May 15, 2017 and May 22, 2017, TANESHA FORD, the defendant, received a total of \$5,141.58 in funds that had been obtained through unauthorized access to an account belonging to a ride-sharing driver, and on or about May 15, 2017 and May 23, 2017, FORD withdrew thousands of dollars in funds from her bank accounts at ATMs located in Pelham, New York.

(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, THALIA CAQUIAS and TANESHA FORD, 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, CAQUIAS and FORD, and others known and unknown, 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 Special Agent with the USSS and I have been personally involved in the investigation of this matter. I have worked on this investigation with Criminal Investigators from the United States Attorney's Office for the Southern District of New York ("USAO SDNY") 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, and alter information in those compromised accounts to divert driver funds to bank accounts controlled by Scheme members.

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.

Overview of the Company-1 Scheme

11. Based on my conversations with representatives from a ride-sharing company ("Company-1"), as well as my review of documents provided by Company-1, I have learned that the fraudulent 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.

d. 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.

e. 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.

f. 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.

g. 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 ride-sharing company ("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 ¶ 24(a), 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, THALIA CAQUIAS and TANESHA FORD, the defendants, appear to have acted primarily as Money Receivers in connection with the Scheme.

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

THALIA CAQUIAS's Participation in the Scheme

18. As set forth in detail below, the investigation has developed evidence indicating that THALIA CAQUIAS, the defendant, participated in the Scheme as a Money Receiver. Evidence of CAQUIAS's involvement in the Scheme includes, among other things, the following: (i) unauthorized transfers from Company-1 and Company-2 into bank accounts held in CAQUIAS's name; (ii) IP addresses registered or otherwise associated with other co-conspirators which are linked to unauthorized transfers from Company-1 sent to CAQUIAS and other Scheme members; (iii) devices connected to other co-conspirators that were involved in making unauthorized transfers sent to CAQUIAS and other Scheme members; and (iv) social media postings by CAQUIAS that indicate CAQUIAS made large cash withdrawals shortly following unauthorized transfers into her bank accounts.

19. Based on my review of bank records obtained in the course of this investigation, my review of records provided by Company-1 and Company-2, and my conversations with a Criminal Investigator from the USAO SDNY ("Investigator-1") who has informed me of his discussions with representatives of Company-1 and Company-2, I have learned that THALIA CAQUIAS, the defendant, received unauthorized transfers from Company-1 and Company-2, as follows:

a. Between on or about November 10, 2016 and on or about February 11, 2017, at least 57 unauthorized transfers were deposited from Company-1 as a result of the Scheme into a TD Bank account held in THALIA CAQUIAS's name ("TD Account-1"), a Bank of America account held in CAQUIAS's name ("BOA Account-1"), and a People's Bank account held in CAQUIAS's name ("People's Bank Account-1"). These unauthorized transfers totaled approximately \$28,816.17.

b. Between on or about July 26, 2017 and on or about September 13, 2017, at least 37 unauthorized transfers were

deposited from Company-2 as a result of the Scheme into BOA Account-1. These unauthorized transfers totaled approximately \$17,791.

c. A review of records for CAQUIAS's bank accounts shows that there were large cash withdrawals and purchases made shortly after the above-described unauthorized transfers were deposited into CAQUIAS's accounts. For example, on or about January 18, 2017, TD Bank Account-1 and BOA Account-1 together received a total of three unauthorized transfers from Company-1 in the amount of approximately \$2,507. On or about January 18, 2017, CAQUIAS withdrew approximately \$1,360 from these accounts. Moreover, on or about January 15, 2017, CAQUIAS received approximately eight unauthorized transfers into her bank accounts from Company-1. On or about January 15, 2017 and on or about January 16, 2017, CAQUIAS withdrew approximately \$1,800 in from those bank accounts at ATMs located in the Bronx, New York.

20. Based on my review of a publicly available Facebook account, bank records, and records provided by Company-1, I have learned that THALIA CAQUIAS, the defendant, made large cash withdrawals from her bank accounts shortly after those accounts received unauthorized transfers from Company-1, as follows:

a. Based on my discussions with Investigator-1, I have learned that Investigator-1 viewed a Facebook account that is believed to belong to THALIA CAQUIAS, the defendant (the "CAQUIAS Facebook Account"). Investigator-1 determined that the CAQUIAS Facebook Account belongs to CAQUIAS based on, among other things, photographs posted on the CAQUIAS Facebook Account that depict an individual that Investigator-1 believes to be CAQUIAS based on Investigator-1's review of photographs contained in law enforcement databases.

b. On or about January 18, 2017, a video was posted by the CAQUIAS Facebook Account depicting a large amount of cash in an individual's hands. As is noted above, see ¶ 19(c), supra; CAQUIAS received unauthorized transfers to her bank accounts from Company-1 on or about January 15, 2017, and withdrew a total of approximately \$1,800 from those accounts on or about January 15, 2017 and on or about January 16, 2017.

c. Furthermore, on or about June 9, 2017, a video was posted by the CAQUIAS Facebook Account depicting CAQUIAS holding a large amount of cash and dancing.

21. Based on my review of telephone provider records, bank account records, and Company-1 records obtained in the course of

this investigation, I have learned, among other things, that the phone number of a co-conspirator ("CC-1")⁴ was used to call approximately 13 Company-1 drivers whose Company-1 accounts were accessed without authorization during the course of the Scheme, resulting in unauthorized transfers of which approximately \$4,523.35 was deposited into a bank account belonging to THALIA CAQUIAS, the defendant.

22. Based on my review of internet provider and Company-1 records obtained in the course of this investigation, I have learned, among other things, that an IP address subscribed to CC-1 that was used to log into driver accounts without authorization is associated with THALIA CAQUIAS, the defendant, as follows:

a. Between on or about October 21, 2016 and on or about February 7, 2017, a specific IP address subscribed to an address in the Bronx, New York that matches the address for CC-1⁵ ("IP-1") was used to log into Company-1 driver accounts without authorization, resulting in approximately 127 unauthorized transfers from Company-1 to Scheme members totaling approximately \$32,089.27. These unauthorized transfers were deposited into bank accounts belonging to CC-1 and THALIA CAQUIAS, the defendant, among others.

b. On or about December 26, 2016, a device connected to IP-1 was used to log into a Company-1 driver's account without authorization, resulting in unauthorized transfers from Company-1 in the amount of approximately \$2,974.21. In addition, according to records obtained from Facebook during the course of this investigation, IP-1 was also used to log into the CAQUIAS Facebook Account on or about December 26, 2016.

23. Based on my review of records provided by Company-1 and my conversation with Investigator-1 regarding his discussions with representatives from Company-1, I have learned, among other things, that devices associated with unauthorized transfers to THALIA CAQUIAS, the defendant, were also associated with unauthorized transfers to other Scheme members, as follows:

⁴Based on my discussions with Investigator-1, I have learned that this phone number is registered to CC-1's Snapchat account.

⁵ Based on my discussions with Investigator-1, I have learned that Investigator-1 determined that this address was associated with CC-1 based on Investigator-1's review of law enforcement databases.

a. Company-1 was able to identify devices with eight unique IDFAs associated with the unauthorized transfers from Company-1 into CAQUIAS's bank accounts.

b. One of those eight IDFAs ("IDFA-1") was linked to approximately 23 unauthorized transfers from Company-1 totaling approximately \$5,863.67. These unauthorized transfers were sent to CAQUIAS's bank accounts, and another co-conspirator ("CC-2"), among others.

c. A second of those eight IDFAs ("IDFA-2") was linked to approximately 26 unauthorized transfers from Company-1 totaling approximately \$6,621.89. These unauthorized transfers were sent to CAQUIAS's bank accounts and CC-1, among others.

d. A third of those eight IDFAs ("IDFA-3") was linked to approximately 69 unauthorized transfers from Company-1 totaling approximately \$31,716.86. These unauthorized transfers were sent to the bank accounts of CAQUIAS, TANESHA FORD, the defendant, and CC-1, among others.

e. A fourth of those eight IDFAs ("IDFA-4") was linked to approximately 53 unauthorized transfers from Company-1 totaling approximately \$15,200.22. These unauthorized transfers were sent to CAQUIAS's bank accounts and CC-2, among others.

24. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that phone numbers used to call drivers as part of the Scheme were associated with unauthorized transfers to THALIA CAQUIAS, the defendant, as well as other Scheme members, as follows:

a. Company-1 identified three phone numbers that were used to call Company-1 drivers shortly before the unauthorized transfers from Company-1 into a bank account at Popular Community Bank held in the name of CC-2 ("Popular Bank Account-1"). I have determined that these phone numbers are all serviced by Pinger, a free service that lets users "spoof," or mask, the number they use to call.

b. One of these telephone numbers ("Pinger Phone Number-1") was also associated with approximately 55 unauthorized transfers from Company-1, including approximately \$615.55 in transfers to TD Account-1, which, as noted above, is held in the name of THALIA CAQUIAS, the defendant.

c. Another of these telephone numbers ("Pinger Phone Number-2") was associated with approximately 37 unauthorized

transfers from Company-1, including transfers in the amount of \$1,447.14 to TD Account-1.

25. Based on my discussions with Investigator-1, I have learned that representatives of Company-1 and Company-2 have respectively informed Investigator-1 that THALIA CAQUIAS, the defendant, has never been employed as a driver by Company-1 and Company-2.

TANESHA FORD's Participation in the Scheme

26. As set forth in detail below, the investigation has developed evidence indicating that TANESHA FORD, the defendant, participated in the Scheme as a Money Receiver. Evidence of FORD's involvement in the Scheme includes, among other things, the following: (i) unauthorized transfers from Company-1 and Company-2 into bank accounts held in FORD's name; (ii) IP addresses registered or otherwise associated with other co-conspirators which are linked to unauthorized transfers from Company-2 sent to FORD and other Scheme members; (iii) devices connected to FORD that were involved in making unauthorized transfers sent to FORD and other Scheme members; and (iv) social media communications in which FORD discusses the Scheme.

27. Based on my review of bank records obtained in the course of this investigation, my review of records provided by Company-1 and Company-2, and my conversations with Investigator-1, who has informed me of his discussions with representatives of Company-1 and Company-2, I have learned, among other things, that TANESHA FORD, the defendant, received unauthorized transfers from Company-1 and Company-2, as follows:

a. Between on or about December 9, 2016 and on or about May 22, 2017, at least 10 unauthorized transfers were deposited from Company-1 as a result of the Scheme into a TD Bank account held in TANESHA FORD's name ("TD Account-2"). These unauthorized transfers totaled approximately \$6,133.63.

b. Between on or about February 15, 2017 and on or about May 22, 2017, at least 39 unauthorized transfers were deposited from Company-2 as a result of the Scheme into TD Account-2. These unauthorized transfers totaled approximately \$22,265.70.

c. A review of records for FORD's TD Account-2 shows that there were large cash withdrawals and purchases made shortly after the above-described unauthorized transfers were deposited into TD Account-2. For example, on or about May 15,

2017 and May 22, 2017, TD Bank Account-2 received a total of \$5,141.58 in unauthorized transfers from Company-1 and Company-2. On or about May 15, 2017, FORD withdrew approximately \$1,000 from TD Account-2 at an ATM located in Pelham, New York. On or about May 23, 2017, FORD withdrew approximately \$3,140 in cash from TD Account-2 at an ATM located in Pelham, New York.

28. Based on my review of records obtained in the course of this investigation, I have learned, among other things, that phone numbers used to call drivers as part of the Scheme were associated with unauthorized transfers to TANESHA FORD, the defendant, as well as other Scheme members, as follows:

a. Company-1 identified a Pinger telephone number ("Pinger Phone Number-3") that was used to call a Company-1 driver shortly before the unauthorized transfer from Company-1 into TD Account-2, which as noted above is held by TANESHA FORD, the defendant. Pinger Phone Number-3 is also linked with at least two additional unauthorized transfers from Company-1 into another Scheme member's account.

29. 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 TANESHA FORD, the defendant, discussed the Scheme with others, as follows:

a. One of the Snapchat accounts searched as part of the WCDAO Search Warrant returns appears to belong to TANESHA FORD, the defendant (the "FORD Snapchat Account"). I have determined that the FORD Snapchat Account is associated with FORD based on, among other things, the email address subscribed to the FORD Snapchat Account, which contains FORD's full name, as well as messages sent from the FORD Snapchat Account in which FORD provided her true date of birth, which matches New York State records, and sent photographs of a debit card bearing FORD's name.

b. An additional Snapchat account searched as part of the WCDAO Search Warrant returns appears to belong to another co-conspirator ("CC-3") (the "CC-3 Snapchat Account"). The photographs in the CC-3 Snapchat Account appear to depict CC-3, based on my review of photographs of CC-3 contained in law enforcement databases.

c. On or about April 5, 2017, the CC-3 Snapchat Account and the FORD Snapchat Account engaged in the following message exchange:

CC-3: I could use ya TD today
FORD: I need My Card That's Where All My Money Is
CC-3: Send the card

d. FORD then sent CC-3 a Snapchat message containing a photograph of a TD Bank Debit Card with FORD's name ("Debit Card-1"), which is associated with TD Account-2. On or about April 10, 2017, there were two unauthorized transfers from Company-2 to Debit Card-1 totaling approximately \$1,024.11.

e. On or about March 5, 2017, the FORD Snapchat Account engaged in the following message exchange with another unidentified individual ("UI"):

UI: I wanna make some coins
UI: Tell that man to teach me that [Company-1]
FORD: Ok

f. On or about April 21, 2017, the FORD Snapchat Account sent a message to another Snapchat user stating, "I'm Blocked From [Company-2]."

30. Based on my review of records provided by Company-1 and my conversation with Investigator-1 regarding his discussions with representatives from Company-1, I have learned, among other things, that devices associated with unauthorized transfers to TANESHA FORD, the defendant, were also associated with unauthorized transfers to other Scheme members, as follows:

a. Company-1 was able to identify devices with at least two unique IDFAs associated with the unauthorized transfers from Company-1 into bank accounts held in the name of TANESHA FORD, the defendant.

b. One of those two IDFAs ("IDFA-4") was linked to approximately 69 unauthorized transfers from Company-1 totaling approximately \$31,716.86. A portion of these unauthorized transfers totaling \$1,455.03 were sent to TD Account-2, which is an account held in FORD's name as described above.

c. The second of those two IDFAs (IDFA-5) was linked to one unauthorized transfer from Company-1 to TD Account-2, as

well as two unauthorized transfers to the account of another Scheme member.

31. Based on my review of internet provider and Company-1 and Company-2 records obtained in the course of this investigation, I have learned, among other things, that an IP address that was used to log into Company-1 and Company-2 driver accounts without authorization is associated with TANESHA FORD, the defendant, as follows:

a. On or about January 29, 2017, February 6, 2017, and February 10, 2017, a specific IP address ("IP-2") was used to log into Company-1 driver accounts without authorization, resulting in unauthorized transfers from Company-1.

b. Based on my review of Company-2 records, I have learned that IP-2 was also used to log into Company-2 driver accounts without authorization on or about March 17, 2017 and on or about April 24, 2017, resulting in unauthorized transfers from Company-2 to a bank account held by TANESHA FORD, the defendant, among others.

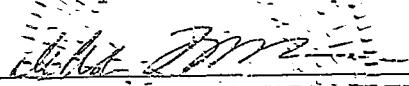
32. Based on my discussions with Investigator-1, I have learned that representatives of Company-1 and Company-2 have respectively informed Investigator-1 that TANESHA FORD, the defendant, has never been employed as a driver by Company-1 and Company-2.

WHEREFORE, deponent respectfully requests that warrants be issued for the arrests of THALIA CAQUIAS and TANESHA FORD, the defendants, and that they be imprisoned or bailed, as the case may be.



TRAVIS WRIGHT
Special Agent
United States Secret Service

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



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