


Approved: 
MICHAEL D. NEFF/BRETT M. KALIKOW
Assistant United States Attorneys

Before: THE HONORABLE BARBARA MOSES
United States Magistrate Judge
Southern District of New York

-----X
: UNITED STATES OF AMERICA :
: : SEALED COMPLAINT
: -v.- :
: :
: ISAAC CONCEPCION AQUINO, : Violations of
: a/k/a "Kaka," : 18 U.S.C. §§ 1349,
: MARIO DIAZ, : 1028A, and 2
: a/k/a "Memin," :
: TOMAS GUILLEN, :
: a/k/a "Diddy," : COUNTY OF OFFENSE:
: RONNIE DE LEON, : BRONX
: JOSE ARGELIS DIAZ, :
: JOEL PENNA, :
: JHONATAN DIAZ, :
: a/k/a "Nino," :
: EDDY MORROBEL, : 18MAG 6622
: RUDDY SANCHEZ, :
: MICHAEL ROQUE, :
: RAYNIEL ROBLES, and :
: JOANDRA TEJADA GONZALEZ, :
: Defendants. :
: :
-----X

SOUTHERN DISTRICT OF NEW YORK, ss.:

GEORGE MURPHY WHALEN, being duly sworn, deposes and says that he is a Task Force Officer with the United States Department of Homeland Security, Homeland Security Investigations ("HSI"), and charges as follows:

COUNT ONE
(Conspiracy to Commit Wire Fraud)

1. From at least in or about 2014 up to and including the present, in the Southern District of New York and elsewhere, ISAAC

CONCEPCION AQUINO, a/k/a "Kaka," MARIO DIAZ, a/k/a "Memin," TOMAS GUILLEN, a/k/a "Diddy," RONNIE DE LEON, JOSE ARGELIS DIAZ, JOEL PENA, JHONATAN DIAZ, a/k/a "Nino," EDDY MORROBEL, RUDDY SANCHEZ, MICHAEL ROQUE, RAYNIEL ROBLES, and JOANDRA TEJADA GONZALEZ, 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 part and an object of the conspiracy that ISAAC CONCEPCION AQUINO, a/k/a "Kaka," MARIO DIAZ, a/k/a "Memin," TOMAS GUILLEN, a/k/a "Diddy," RONNIE DE LEON, JOSE ARGELIS DIAZ, JOEL PENA, JHONATAN DIAZ, a/k/a "Nino," EDDY MORROBEL, RUDDY SANCHEZ, MICHAEL ROQUE, RAYNIEL ROBLES, and JOANDRA TEJADA GONZALEZ, 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 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

(Aggravated Identity Theft)

3. On or about October 4, 2015, in the Southern District of New York and elsewhere, ISAAC CONCEPCION AQUINO, a/k/a "Kaka," the defendant, 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, in or around New York, New York, CONCEPCION AQUINO possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint.

(Title 18, United States Code, Section 1028A.)

COUNT THREE

(Aggravated Identity Theft)

4. On or about September 22, 2014, in the Southern District of New York and elsewhere, MARIO DIAZ, a/k/a "Memin," the defendant, 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, in or around Greensboro, North Carolina,¹ DIAZ possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint.

(Title 18, United States Code, Section 1028A.)

COUNT FOUR

(Aggravated Identity Theft)

5. On or about August 16, 2016, in the Southern District of New York and elsewhere, TOMAS GUILLEN, a/k/a "Diddy," the defendant, 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, in or around New York, New York, GUILLEN possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint, and aided and abetted the same.

(Title 18, United States Code, Sections 1028A and 2.)

COUNT FIVE

(Aggravated Identity Theft)

6. On or about December 5, 2017, in the Southern District of New York and elsewhere, RONNIE DE LEON, the defendant, 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,

¹ See, e.g., *United States v. Magassouba*, 619 F.3d 202, 203 (2d Cir. 2010) ("On appeal, [the defendant] argues that the government failed to prove venue in the Southern District of New York by a preponderance of the evidence with respect to the aggravated identity theft count, because there was no evidence that he transferred, possessed, or used another person's means of identification within that district. We disagree, and hold that where (as here) venue is appropriate for the predicate felony offense, so too is venue appropriate for a prosecution of the separate crime of knowingly transferring, possessing, or using a means of identification of another person 'during and in relation to' that offense.").

Section 1028A(c), to wit, DE LEON possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint, resulting in DE LEON's arrest that day in or around Wauwatosa, Wisconsin.

(Title 18, United States Code, Section 1028A.)

COUNT SIX

(Aggravated Identity Theft)

7. On or about November 13, 2017, in the Southern District of New York and elsewhere, JOSE ARGELIS DIAZ, the defendant, 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, in or around Las Cruces, New Mexico, DIAZ possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint, and aided and abetted the same.

(Title 18, United States Code, Sections 1028A and 2.)

COUNT SEVEN

(Aggravated Identity Theft)

8. On or about December 22, 2017, in the Southern District of New York and elsewhere, JOEL PENA, the defendant, 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, in or around Danvers, Massachusetts, PENA possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint.

(Title 18, United States Code, Section 1028A.)

COUNT EIGHT

(Aggravated Identity Theft)

9. On or about June 18, 2016, in the Southern District of New York and elsewhere, JHONATAN DIAZ, a/k/a "Nino," the defendant, 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, in or around San Diego, California, DIAZ possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint, and aided and abetted the same.

(Title 18, United States Code, Sections 1028A and 2.)

COUNT NINE

(Aggravated Identity Theft)

10. On or about May 28, 2017, in the Southern District of New York and elsewhere, EDDY MORROBEL, the defendant, 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, in or around the Bronx, New York, MORROBEL possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint.

(Title 18, United States Code, Section 1028A.)

COUNT TEN

(Aggravated Identity Theft)

11. On or about March 18, 2017, in the Southern District of New York and elsewhere, RUDDY SANCHEZ, the defendant, 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, in or around Long Beach, California, SANCHEZ possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint.

(Title 18, United States Code, Section 1028A.)

COUNT ELEVEN

(Aggravated Identity Theft)

12. On or about May 17, 2017, in the Southern District of New York and elsewhere, MICHAEL ROQUE, the defendant, 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, ROQUE possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint, which resulted in his arrest in or around Glendale, California.

(Title 18, United States Code, Section 1028A.)

COUNT TWELVE

(Aggravated Identity Theft)

13. On or about July 10, 2017, in the Southern District of New York and elsewhere, RAYNIEL ROBLES, the defendant, 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, in or around Akron, Ohio, ROBLES possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint.

(Title 18, United States Code, Section 1028A.)

COUNT THIRTEEN

(Aggravated Identity Theft)

14. On or about July 18, 2017, in the Southern District of New York and elsewhere, JOANDRA TEJADA GONZALEZ, the defendant, 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, GONZALEZ possessed, used, and transferred the name and other personal identification information of another person in connection with the wire fraud conspiracy, as charged in Count One of this Complaint, which resulted in her arrest in or around Flowood, Mississippi.

(Title 18, United States Code, Section 1028A.)

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

15. I am a Task Force Officer ("TFO") with HSI and I have been personally involved in the investigation of this matter. This

affidavit is based upon my personal participation in the investigation, my examination of reports, records, seized evidence, and photographs, and my conversations with other law enforcement officers and other individuals. 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.

Terminology

16. Based on my training, research, education, and experience, I am familiar with the following relevant terms:

a. The "dark web" is a colloquial name for a number of extensive, sophisticated, and widely used criminal marketplaces operating on the Internet. These marketplaces allow participants to buy and sell illegal items -- such as drugs, guns, fraudulent identifications, personal identification information ("PII") stolen from victims, computer hacking tools, and other hazardous materials -- with greater anonymity than is possible on the traditional Internet. These online black market websites use a variety of technologies, including the Tor network (defined below) and other encryption technologies, to ensure that communications and transactions are shielded from interception and monitoring.

b. The "Tor network," or simply "Tor," is a special network of computers on the Internet, distributed around the world, that is designed to conceal the true Internet Protocol ("IP") addresses of the computers accessing the network and, thereby, the locations and identities of the network's users. Tor likewise enables websites to operate on the network in a way that conceals the true IP addresses of the computer servers hosting the websites, which are referred to as "hidden services." Such "hidden services" operating on Tor have complex web addresses, generated by a computer algorithm, ending in ".onion" and can only be accessed through specific web browser software, including a major dark-web browser known as "Tor Browser," designed to access the Tor network.

c. "Bitcoin" (or "BTC") is an online digital currency that allows users to transfer funds with greater anonymity than would be possible through traditional banking and credit systems. Users store their bitcoins in digital "wallets," which are identified by unique electronic "addresses." Although

Bitcoins are legal and have known legitimate uses, cybercriminals often use Bitcoins for money-laundering purposes. Bitcoins are believed to be the most oft-used means of payment for illegal goods and services on "dark web" websites operating on the Tor network. By maintaining multiple bitcoin wallets, those who use bitcoins for illicit purposes can attempt to thwart law enforcement's efforts to track purchases within a dark web marketplace. As of August 2, 2018, one bitcoin was worth approximately \$7,544.79, though bitcoins' value is much more volatile than that of fiat currencies.

d. An International Mobile Equipment Identity ("IMEI") number is a unique numerical code associated with each cellphone or mobile device. A device's IMEI number can be necessary to unlock the device from a particular cellular service company or to use an insurance policy.

e. A subscriber identity module or subscriber identification module ("SIM") is an integrated circuit chip that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers, including for cellphones.

Overview of the Fraud Schemes

17. Since in or around 2016, HSI has been investigating a group of individuals -- the "Fraud Ring" -- that operated in the Southern District of New York (the Bronx, Manhattan, Mt. Vernon, etc.) and the Dominican Republic, among other places. From at least 2014 to the present, the Fraud Ring perpetrated a wide-ranging scheme to obtain valuable, new electronic devices -- primarily but not exclusively iPhones -- at others' expense. During the course of the conspiracy, the Fraud Ring fraudulently obtained more than \$1 million worth of devices. To facilitate the scheme, the Fraud Ring traveled to at least approximately 30 different states, but often brought or shipped the fraudulently obtained cellphones back to the Bronx, where they regularly sold them through fencing operations.

18. The Fraud Ring regularly engaged in intrusions into existing customers' accounts with cellular service companies in order to obtain iPhones and, less frequently, other valuable goods and devices including iPads, tablets, and watches. The Fraud Ring frequently obtained new phones or "upgrade" phones by paying only a small fee in the store, while charging the vast majority of the purchase price to existing customers' accounts, without the consent or knowledge of these existing customers. In addition to

exploiting existing customers' accounts, at times the Fraud Ring also created new fraudulent accounts. Thus, the scheme's victims include (1) customers, whose identities were stolen and/or whose accounts were accessed without authorization; and (2) cellphone service providers, which typically bore financial losses inflicted by the scheme.

19. Over time, the Fraud Ring used various mechanisms to perpetrate their scheme. They changed their precise mechanisms in an attempt to stay ahead of law enforcement. Some of the mechanisms used by the Fraud Ring include the following:

a. Buying PII over the Dark Web: The Fraud Ring used Bitcoin to purchase cellphone customers' PII over the dark web and then used that information to convince stores (which sell cellphones) that the co-conspirators were, in fact, the legitimate owners or users of the cellphone account, thereby inducing the stores into supplying the co-conspirators with new or upgraded cellphones;

b. Phishing/Hacking: The Fraud Ring emailed a link to cellphone customers and, if the customer opened this link, it enabled the co-conspirators to hack that customer's account, change the authorized user(s) on the victim's account, and then obtain phones charged to that account;

c. Fraudulent IDs: The Fraud Ring used fraudulent identification to persuade retail store employees that the conspirator was, in fact, someone else; and

d. Social Security Fraud: The Fraud Ring purchased phones using their real names and a social security number that appeared to (and sometimes did) match the spelling of their real names, but in fact the social security number belonged to someone else, thereby damaging someone else's credit.

Search Warrant Executed on a Hub of the Fraud Ring

20. Based on my participation in this investigation, I know that a judicially authorized search warrant (the "Warrant") was executed on or about August 15, 2017 at a residence in Mt. Vernon, New York (the "Mt. Vernon Residence"). The Mt. Vernon Residence was believed, at that time, to be the hub of the Fraud Ring. Based on my participation in this investigation, my participation in the execution of the Warrant, my conversations with others, and my review of documents, reports, and photographs, I have learned the following, among other things:

a. Two IP addresses associated with the Mt. Vernon Residence were used to access at least approximately 3,300 customer accounts of a cellphone service company ("Cellphone Company-1"), including approximately 492 compromised customer accounts that were exploited such that others fraudulently purchased approximately 1,294 cellphones.

b. During execution of the Warrant, six of the defendants named in this Complaint -- defendants ISAAC CONCEPCION AQUINO, a/k/a "Kaka," MARIO DIAZ, a/k/a "Memin," JOSE ARGELIS DIAZ, JHONATAN DIAZ, a/k/a "Nino," EDDY MORROBEL, and RUDDY SANCHEZ -- were present in the Mt. Vernon Residence. In addition, a temporary vehicle registration for "RONNIE DELEON" was found in the Mt. Vernon Residence.

c. During execution of the Warrant, law enforcement seized, among other things, at least approximately twelve computers, approximately five iPads, and approximately thirty cellphones, two of which were brand new iPhones that were in clear plastic wrapping, and appeared to have been shipped by FedEx. Law enforcement also seized, among other things, receipts for Western Union and MoneyGram transactions; a Bitcoin transaction; and transactions at various banks (e.g., Bank of America, JPMorgan Chase, and Capital One). Also present at the Mt. Vernon Residence were several standalone SIM cards.

d. As further detailed below, the computers seized during the execution of the Warrant contained various indicators that the computers were used by the Fraud Ring in furtherance of their scheme, including, among other things:

i. A 15-minute long "How-to" video (in Spanish), which details the steps necessary to commit cellphone fraud, including how to use victim PII to access victim accounts and fraudulently purchase devices (the "How-to Video");

ii. Numerous internet searches for terms such as "at&t my order status," "Verizon claim," "best buy check my upgrade," "federal tax id number buy," "liberar imei de verizon" (which translates to "release imei from Verizon"), and the names of various credit and background check websites; and

iii. Indicators that computers accessed various darkweb sites, including the Tor browser, several websites where PII is sold, and Bitcoin and other cryptocurrency exchanges.

21. During the search of the Mt. Vernon Residence, approximately seven occupants spoke with law enforcement. Several

occupants of the Mt. Vernon Residence said they were all friends who were in New York from the Dominican Republic.

22. The search of the Mt. Vernon Residence occurred a few weeks after an individual ("CW-1")² went to the Mt. Vernon Residence. CW-1 told me the following, among other things:

a. CW-1 saw four people working at laptop computers and several others watching television. CW-1 recognized two of these four individuals as people with whom CW-1 had previously engaged in cellphone fraud.

b. While CW-1 was at the Mt. Vernon Residence, a resident asked CW-1 if CW-1 could get them a "worker," which CW-1 understood to mean a participant who could assist in the cellphone fraud scheme.

c. While CW-1 was at the Mt. Vernon Residence, CW-1 saw approximately two iPhone boxes.

d. CW-1 also saw that one of the individuals working on a laptop computer appeared to have Gmail up on the screen. CW-1 heard one individual say, in Spanish, and in sum and substance, "You can go ahead, I already got the confirmation. The account is ready."

RONNIE DE LEON

23. Based on, among other things, my review and analysis of documents and reports provided by Cellphone Company-1, I have learned the following about RONNIE DE LEON, the defendant:

a. Between approximately April 7, 2017 and December 5, 2017, DE LEON's name, derivatives thereof (e.g., "Ronnie Deleon," "Ronnie C. De Leon," "Ronnie C. Deleon," "Ronnie Cecilio De Leon"), or his address in San Antonio, Texas (the "DE LEON Texas Address"), or his address in Galloway, Ohio (the "DE LEON Ohio Address") were used in connection with approximately 100 compromised accounts of

² CW-1 is a former participant in the Fraud Ring. CW-1 has previously been convicted of a felony and of violations of supervised release. By cooperating with the Government over a period of time, CW-1 has hoped to obtain a benefit, initially at sentencing, thereafter in the form of payment in exchange for information. The information CW-1 has provided the Government throughout has been reliable, and has been corroborated by independent evidence, including information supplied by other cooperating witnesses who also participated in the Fraud Ring.

Cellphone Company-1.³ Each of these approximately 100 accounts was a victim of fraudulent cellphone purchases.

b. Approximately 405 cellphones were obtained on these approximately 100 compromised accounts.

c. This fraudulent activity, which appears to be attributable to DE LEON, caused at least approximately \$366,183.03 in losses to Cellphone Company-1.⁴

24. Based on, among other things, my review and analysis of documents and reports provided by another company that provides cellphone service ("Cellphone Company-2"), I have learned the following about RONNIE DE LEON, the defendant:

a. From in or about June 2017 through in or about August 2017, DE LEON's name, or derivatives thereof (e.g., "Ronnie Deleon" or "Ronie Deleon"), were used in connection with approximately six compromised accounts of Cellphone Company-2 customers located in California, Arizona, and Texas, resulting in approximately 17 fraudulently obtained cellphones.

b. The email addresses added to these compromised accounts included the following:

- i. r.d.e.le.on.[four numbers]@gmail.com
- ii. r.deleo.n2.[three numbers]@gmail.com
- iii. rdeleon[four numbers]@gmail.com
- iv. r.d.el.eo.n.[four numbers]@gmail.com

³ DE LEON's Texas Address was listed on his Texas Driver's License and DE LEON's Ohio Address was listed on his Ohio Driver's License. Both of these driver's licenses were photographed in connection with DE LEON's arrest, following his fraudulent purchase of a cellphone in Wauwatosa, Wisconsin, which is detailed below.

⁴ When a victim customer informs Cellphone Company-1 that s/he did not make the purchase at issue, Cellphone Company-1 endures the cost and thus the loss.

Because the investigation is ongoing, these approximate loss amounts are preliminary and may change, including if, for instance, it becomes clear that a scheme participant used an additional alias to fraudulently obtain additional cellphones.

v. r.d.e.l.e.o.n[four numbers]@gmail.com

c. This fraudulent activity, which appears to be attributable to DE LEON, caused at least approximately \$12,068.80 in losses to Cellphone Company-2, which -- similar to Cellphone Company-1 -- typically endures the cost and thus the loss.

25. Based on, among other things, my conversations with law enforcement and my review of reports provided by Cellphone Company-1, I have learned the following:

a. On or about December 2, 2017, a fraudulent iPhone purchase was made at a store in Roseville, Minnesota ("Store-1").

b. On the same day at approximately 4:08pm, the billing address of a Cellphone Company-1 customer ("Victim-1") was changed from Victim-1's address to the DE LEON Texas Address.

c. On the same day at approximately 4:09pm, the name of RONNIE DE LEON, the defendant, was added as a purportedly authorized user to Victim-1's account with Cellphone Company-1. Shortly thereafter, a security PIN code sent to Victim-1's billing email address was verified inside of Store-1.

d. Cellphone Company-1 contacted Store-1 and verified that DE LEON was in Store-1 attempting to purchase an iPhone.

e. DE LEON purchased an iPhone for approximately \$949 and left the store before police arrived.

f. Victim-1 told Cellphone Company-1 that Victim-1 neither knew DE LEON nor authorized DE LEON's purchase.

26. Based on, among other things, conversations with law enforcement, reviews of Wauwatosa Police Department reports, and my review of photographs, I have learned, among other things, the following:

a. On or about December 5, 2017, at a particular store in Wauwatosa, Wisconsin ("Store-2"), RONNIE DE LEON, the defendant, purchased a silver iPhone 8 plus, the cost of which was primarily charged to someone else, a Cellphone Company-1 customer ("Victim-2").

b. On or about that same date, Victim-2's billing address (with Cellphone Company-1) was changed from Victim-2's address to the DE LEON Texas Address.

c. On or about that same date, DE LEON's name was added as a purportedly authorized user on Victim-2's account (with Cellphone Company-1).

d. A PIN verification was sent to Victim-2's email address, which was verified inside of Store-2.

e. Cellphone Company-1 contacted Store-2 and confirmed that DE LEON was attempting to purchase an iPhone using Victim-2's account.

f. At Store-2, DE LEON purchased a silver iPhone 8 plus for approximately \$949 using Victim-2's account.

g. DE LEON was arrested as he was leaving Store-2.

h. Victim-2 confirmed that Victim-2 neither knew DE LEON nor authorized DE LEON's purchase.

27. Based on, among other things, my review of criminal history records in a law enforcement database, I know that RONNIE DE LEON, the defendant, ultimately pled guilty, under Wisconsin state law, to unauthorized use of an individual's identity.

28. Based on, among other things, my conversations with law enforcement in Wisconsin, I have learned that RONNIE DE LEON, the defendant, was using a rental car with a particular license plate number (the "Rental License Plate") at the time of his Wisconsin arrest. Based on my review of license plate reader information, I know that the Rental License Plate was in Minnesota on or about both December 1 and December 2, 2017. For instance, on or about December 2, 2017, the Rental License Plate was in Bloomington, Minnesota, which is approximately a 20-minute drive from Roseville, Minnesota, where the December 2, 2017 fraudulent purchase of an iPhone took place using DE LEON's name and the DE LEON Texas Address on Victim-1's account.

29. Based on my review of Wauwatosa Police Department documents, reports, and photographs, I have learned the following, among other things:

a. On or about December 5, 2017, in connection with his arrest in Wauwatosa, Wisconsin, law enforcement seized a cellphone from RONNIE DE LEON, the defendant (the "De Leon Cellphone").

b. The De Leon Cellphone was on at the time it was seized. The De Leon Cellphone received messages and emails,

portions of which were visible on the home screen, without unlocking the phone (*i.e.*, the De Leon Cellphone was receiving "notifications" that were visible in plain view).

c. There were portions of email messages from Cellphone Company-1 visible on the home screen of the De Leon Cellphone, notifying DE LEON of profile and account updates for two Cellphone Company-1 customers, one of whose first names matched the first name of Victim-2.

d. These messages were dated December 5, 2017, the same day that DE LEON was arrested for fraudulently purchasing an iPhone using Victim-2's account.

e. The De Leon Cellphone's home screen revealed that it had received text messages and calls, via the Snapchat application, from "Diddy2020."⁵

i. "Diddy2020" is believed to be the Snapchat account of a co-defendant, TOMAS GUILLEN, a/k/a "Diddy."

ii. Based on my conversations with CW-1, I know, among other things, that GUILLEN's nickname is "Diddy," and that GUILLEN resided at a particular address in the Bronx beginning with "2020", an address that was formerly a hub of this conspiracy.⁶

30. Based on my review of documents provided by Western Union, I have learned, among other things, that in between on or about June 16, 2017 and on or about May 21, 2018, RONNIE DE LEON, the defendant, sent wire transfers totaling approximately \$3,000 to a suspected co-conspirator in the Dominican Republic ("CC-3"), whom I understand from CW-1 has been arrested. DE LEON sent one

⁵ Based on my training, experience, and review of publicly available information, I know that Snapchat is a multimedia messaging application in which messages and photographs are available for only a limited period, before they become inaccessible.

⁶ As explained below, based on my involvement in this investigation, including my review of a Glendale, California Police Department report, I have learned, among other things, that RONNIE DE LEON, the defendant, was also arrested on or about May 17, 2017, in Glendale, California, on charges of theft, burglary, and identity theft, stemming from his purchase of approximately five iPhone 7Plus cellphones on others' accounts (two at an Apple store in Pasadena, California, and three at an Apple store in Glendale, California).

transfer from in or around Columbus, Ohio, and the other from in or around the Bronx, New York. For both wire transfers, DE LEON provided the DE LEON Ohio Address as the sender address.

a. As noted below, other co-defendants also sent four-figure wire transfers to CC-3 as well, such as TOMAS GUILLEN, a/k/a "Diddy," and MARIO DIAZ, a/k/a "Memin."

TOMAS GUILLEN, a/k/a "Diddy"

31. Based on my review and analysis of documents and reports prepared by Cellphone Company-1, I have learned, among other things, the following about TOMAS GUILLEN, a/k/a "Diddy," the defendant:

a. Between in or about 2015 and the present, GUILLEN's name, or derivatives thereof, were used in connection with approximately 28 compromised Cellphone Company-1 accounts that were used to fraudulently obtain approximately 53 cellphones.

b. The billing addresses of approximately 11 Cellphone Company-1 accounts were changed to a particular address in the Bronx, New York (the "GUILLEN Address"), which is a known address of GUILLEN's based on, among other things, criminal history records.

c. This fraudulent activity, which appears to be attributable to GUILLEN, caused approximately \$48,507.89 in losses to Cellphone Company-1.

32. Based on my review and analysis of documents and reports prepared by Cellphone Company-2, I have learned, among other things, the following about TOMAS GUILLEN, a/k/a "Diddy," the defendant:

a. In or around 2014, approximately 12 accounts were compromised of customers in Kentucky, Massachusetts, Maryland, Vermont, and Virginia. These compromised accounts are associated with the fraudulent purchase of approximately 43 cellphones. Each of the approximately 43 fraudulently obtained cellphones was linked to GUILLEN's name, or derivatives thereof.

b. The email address tomasaguillen[two numbers]@hotmail.com was associated with at least approximately three of these compromised accounts. The customer address listed for these same three compromised accounts was the GUILLEN Address.

c. This fraudulent activity, which appears to be attributable to GUILLEN, caused approximately \$30,752.36 in losses to Cellphone Company-2.

33. On or about November 2017, CW-1 told me, in substance and in part, that a package (the "Package") was being sent by RONNIE DE LEON, the defendant, to TOMAS GUILLEN, a/k/a "Diddy," the defendant, via a particular FedEx store in New Jersey (the "Location"). CW-1 added, in substance and in part, that the Package contained approximately 20 new fraudulently obtained iPhone 8 cellphones.

34. Another agent and I established surveillance outside the Location, where I observed the following, among other things:

a. An individual later identified as GUILLEN entered the Location not holding a package, but exited the Location holding a package.

b. GUILLEN placed the package in a car (the "Car") and entered the Car.

c. The driver of the Car drove away from the Location with GUILLEN in the Car as a passenger.

35. Another agent and I followed GUILLEN from the Location as the Car traveled from New Jersey into the Bronx. In the Bronx, we conducted a lawful car stop, obtained GUILLEN's express permission to search his vehicle, and seized the Package. The Package was addressed from "Ronnie De Leon," whose sender address was the DE LEON Texas Address; the Package was addressed to "Tomas Guillen". The Package contained approximately 17 new iPhone 8 cellphones. A brief conversation ensued with GUILLEN, during which the following was said, in substance and in part:

a. GUILLEN admitted that the Package was his and said it contained phones.

b. GUILLEN agreed with my assessment that the phones were likely obtained by fraud.

c. GUILLEN said he sells the phones when he receives them.

d. GUILLEN requested to keep one of the phones in the Package. His request was declined.

36. Based on, among other things, my review and analysis of reports provided by Cellphone Company-1, I have learned that all 17 iPhones in the Package were purchased through compromised Cellphone Company-1 accounts, at least two of which were closed for fraud; all 17 iPhones are associated with the name RONNIE DE LEON, the defendant; and all 17 iPhones were obtained fraudulently.

37. Based on, among other things, conversations with CW-1, I have learned the following, in substance and in part:

a. TOMAS GUILLEN, a/k/a "Diddy," the defendant, had previously paid CW-1 for his participation in the scheme. For example, in or around June 2015, CW-1 and GUILLEN went to a store together to sell approximately 30 fraudulently obtained iPhones. CW-1 communicated with GUILLEN via FaceTime and WhatsApp.⁷

b. CW-1 and GUILLEN worked with at least one co-conspirator located in the Dominican Republic ("CC-1"). GUILLEN traveled back and forth between New York City and the Dominican Republic. GUILLEN would bring cash to CC-1 in the Dominican Republic.

c. GUILLEN would also travel to Georgia, Alabama, and North Carolina because stores in those locations were perceived by the Fraud Ring to be less sophisticated in identifying and preventing fraudulent purchases than stores in New York City. In or around August 2017, GUILLEN travelled to Texas and returned with approximately 88 cellphones. GUILLEN obtained approximately \$60,000 from that trip.

d. ISAAC CONCEPCION AQUINO, a/k/a "Kaka," the defendant, would send GUILLEN customer account information.

e. GUILLEN used Western Union and MoneyGram transfers in furtherance of the scheme.

38. Based on, among other things, my review of records provided by MoneyGram, I have learned that, between in or about 2017 and the present, TOMAS GUILLEN, a/k/a "Diddy," the defendant, sent approximately 73 wire transfers from San Antonio, Texas to Honduras. All but three of those transfers were to individuals who had the same last name as GUILLEN. Based on my involvement in this investigation, I believe that with these wire transfers,

⁷ Based on my training, experience, and review of publicly available information, I know that WhatsApp uses end-to-end encryption and touts the secure nature of communications on this application.

GUILLEN was sending the proceeds of the fraudulent cellphone purchases to relatives in Honduras.

39. Based on my review of Western Union records and reports, I have learned, among other things, that during the course of the charged conspiracy, TOMAS GUILLEN, a/k/a "Diddy," the defendant, sent wire transfers totaling approximately \$22,327 to ISAAC CONCEPCION AQUINO, a/k/a "Kaka," the defendant. Based on my involvement in this investigation, I believe that GUILLEN was paying CONCEPCION for victims' PII in furtherance of the scheme.

MICHAEL ROQUE

40. Based on my review and analysis of documents and reports prepared by Cellphone Company-1, I have learned, among other things, the following about MICHAEL ROQUE, the defendant:

a. Between on or about December 31, 2016 and on or about August 7, 2017, ROQUE's name, or derivatives thereof, were used in connection with approximately 43 compromised Cellphone Company-1 accounts in California, Texas, Ohio, Colorado, Utah, Missouri, and Oregon. These compromised accounts were used to fraudulently obtain approximately 113 cellphones.

b. The billing addresses of approximately 38 of these compromised Cellphone Company-1 accounts (which were exploited to fraudulently obtain approximately 89 cellphones) were changed to a particular address in Kissimmee, Florida, which is known -- from, among other things, arrest records and a Florida State Driver's License -- to be an address of ROQUE's.

c. This fraudulent activity, which appears to be attributable to ROQUE, caused approximately \$104,936.70 in losses to Cellphone Company-1.

d. For approximately 34 of the fraudulently obtained cellphones for which ROQUE's name was added to an existing customer's account, that customer's account was accessed by one or more of the two IP addresses associated with the Mt. Vernon Residence.

41. Based on my involvement in this investigation, including my review of a Glendale, California Police Department report, I have learned, among other things, the following:

a. MICHAEL ROQUE, the defendant, and RONNIE DE LEON, the defendant, were arrested on or about May 17, 2017, in Glendale, California, on charges of theft, burglary, and identity theft,

stemming from their purchases that day of several iPhone 7Plus cellphones on others' accounts.

b. DE LEON purchased two iPhone 7Plus cellphone at an Apple store in Pasadena, California, and three more at an Apple store in Glendale, California.

c. ROQUE bought two iPhone 7Plus cellphones as upgrades and financed the cellphones on an existing customer's account; ROQUE represented that he was a secondary purchaser on that account. ROQUE also requested two new phone numbers.

d. Law enforcement followed ROQUE as he left the Apple store in Glendale, California carrying the two new cellphones he had just purchased.

e. ROQUE was ultimately arrested, waived his *Miranda* rights, and admitted, in substance and in part, the following:

i. He was working with DE LEON, whose photo he identified.

ii. He was making fraudulent purchases on Cellphone Company-1 accounts.

iii. He worked for "a group of Arabs" based in New York, which texts him account numbers and adds him to accounts.

iv. He had made approximately \$18,000 the prior month from this fraud scheme.

v. He drives the phones to New York.

vi. The cellphones are later shipped to the Middle East, where they are sold for three to four times their (U.S. retail) value.

vii. He identified the location, make, and model of the car that he and DE LEON had been using that day.

1. Officers went to that location, identified the car, and found, among other things, five cellphones (located under a seat) which DE LEON had fraudulently purchased.

2. My review of records from Cellphone Company-1 has confirmed that, on or about May 17, 2017, "Ronnie Deleon," whom I believe to be DE LEON, fraudulently obtained three iPhone 7Plus cellphones from an Apple store in Glendale, California, and two more at an Apple store in Pasadena, California.

JOANDRA TEJADA GONZALEZ and JOSE ARGELIS DIAZ

42. Based on my review and analysis of a report from Cellphone Company-1, I have learned, among other things, the following:

a. Between on or about April 20, 2017 and on or about July 18, 2017, the name of JOANDRA TEJADA GONZALEZ, the defendant, or derivatives thereof, were used in connection with approximately 16 compromised Cellphone Company-1 accounts. Each of these accounts fell victim to fraudulent cellphone purchases.

b. Approximately 32 cellphones were fraudulently obtained on these approximately 16 compromised accounts.

c. Approximately seven of these accounts had their billing addresses changed to an address in Hazleton, Pennsylvania associated with GONZALEZ based on, among other things, Pennsylvania State records (the "Hazleton Address"); approximately six of these accounts had their billing address changed to an address in Cleveland, Ohio associated with GONZALEZ based on, among other things, criminal history records (the "Cleveland Address").

e. For approximately five of these compromised accounts, phone calls from a phone number believed to belong to GONZALEZ (the "GONZALEZ Cellphone Number") were received by Cellphone Company-1 on the same day that GONZALEZ's name was added to those accounts, or within 24 hours of her name being added.⁸

f. For six of the accounts to which GONZALEZ's name was added as a purportedly authorized user, an IP address associated with the Mt. Vernon Residence was used to access those accounts.

g. This fraudulent activity, which appears to be attributable to GONZALEZ, caused approximately \$27,539.68 in losses to Cellphone Company-1.

⁸ According to Cellphone Company-1, the GONZALEZ Cellphone Number is listed as Joandra Tejada Gonzalez's number in a database and is billed to an individual with the last name of "Tejada" (but with a different first name). In addition, the GONZALEZ Cellphone Number is listed on her application for a Pennsylvania State initial identification card. Moreover, the GONZALEZ Cellphone Number is listed as her phone number on both Western Union and MoneyGram wire transfers.

43. Based on my conversations with law enforcement and my review of reports and documents, I have learned the following, among other things:

a. On or about July 18, 2017, JOANDRA TEJADA GONZALEZ, the defendant, was arrested by law enforcement at an AT&T store in Mississippi. GONZALEZ was attempting to fraudulently purchase approximately three iPhone pluses and an Apple watch.

b. On or about August 14, 2017, GONZALEZ waived her *Miranda* rights and admitted to law enforcement, in substance and in part, that:

i. She had used stolen PII of victims to make in-store purchases of cellphones, iPhones, iPads, iWatches, and other digital devices.

ii. She was recruited to the fraudulent scheme by her boyfriend, Jose Diaz (whom I believe to be JOSE ARGELIS DIAZ, the defendant), who taught GONZALEZ how to use victims' PII to enter stores and make purchases with compromised Cellphone Company-1 accounts.

iii. GONZALEZ typically would be driven by an individual to various retail stores, and after GONZALEZ purchased a specific number of electronic devices using victims' PII, typically ten cellphones, the driver would mail the phones, via FedEx, to Jose Diaz in New York (whom I again believe to be JOSE ARGELIS DIAZ, the defendant).

iv. GONZALEZ was transported by Jose Diaz (whom I again believe to be JOSE ARGELIS DIAZ, the defendant) to a Best Buy store in Allentown, Pennsylvania for the purpose of purchasing various digital devices.

v. Jose Diaz (whom I again believe to be JOSE ARGELIS DIAZ, the defendant) would text victim PII to GONZALEZ via WhatsApp. He acquired the victim PII from his younger brother, who resides in the Dominican Republic.

vi. GONZALEZ was paid approximately \$1,800 via Western Union and MoneyGram by Jose Diaz (whom I again believe to be JOSE ARGELIS DIAZ, the defendant) for her involvement in the fraudulent scheme. GONZALEZ believed Jose Diaz resided in Yonkers, New York.

vii. For instance, on or about April 14, 2017, Jose Diaz told GONZALEZ to bring her passport, green card, and proof of

address. On that day, GONZALEZ was taken by a driver to an AT&T store, a Best Buy, and a Target store to make fraudulent purchases of various digital devices utilizing PII provided to her by Jose Diaz (whom I again believe to be JOSE ARGELIS DIAZ, the defendant).

44. Based on my review and analysis of records provided by Western Union and MoneyGram, I have learned, among other things, the following:

a. Between in or around April and July 2017, JOANDRA TEJADA GONZALEZ, the defendant, and JOSE ARGELIS DIAZ, the defendant, repeatedly sent each other wire transfers, which cumulatively contained, among other things, the following information: the Hazleton Address; the Cleveland Address; the GONZALEZ Cellphone Number; a date of birth associated with GONZALEZ (based on, among other things, criminal history records); a particular Dominican Republic passport number, which is associated with JOSE DIAZ; a phone number associated with JOSE DIAZ; and a date of birth associated with JOSE DIAZ.

b. One of the wire transfers was sent from a Mt. Vernon, New York address, located approximately one mile from the Mt. Vernon Residence.

45. Based on my review and analysis of documents and reports prepared by Cellphone Company-2, I have learned, among other things, the following about JOSE ARGELIS DIAZ, the defendant:

a. Between in or about December 2013 and in or about November 2017, the name of JOSE DIAZ, or derivatives thereof, were used in connection with approximately nine compromised accounts of Cellphone Company-2 customers in Texas, Florida, California, New Mexico, and Washington, D.C. These compromised accounts are associated with the fraudulent purchase of approximately 40 cellphones.

b. The email addresses associated with at least approximately six of these compromised accounts are:

- i. Jrdiaz[four numbers]@gmail.com
- ii. mr.josediaz[number]@gmail.com
- iii. josediaz[two numbers]@gmail.com

c. This fraudulent activity, which appears to be attributable to JOSE DIAZ, caused at least approximately \$9,679.94 in losses to Cellphone Company-2.

46. Based on my participation in this investigation, the execution of the Warrant, as well as my conversations with others and my review of documents, reports, and photographs, I have learned the following, among other things:

a. During the execution of the Warrant, JOSE ARGELIS DIAZ, the defendant, was present in the Mt. Vernon Residence, and his Dominican Republic Passport was photographed. He informed law enforcement, among other things, that his wife was "Joandra Tejada," whom I believe to be JOANDRA TEJADA GONZALEZ, the defendant.

b. During the execution of the Warrant, a temporary vehicle registration for "RONNIE DELEON" was found in the room where JOSE DIAZ was staying.

c. At least one computer seized during the execution of the Warrant was used by JOSE DIAZ ("Computer-1"). Computer-1 contained repeated Google Maps searches for both the Hazleton Address -- where his girlfriend or wife, JOANDRA TEJADA GONZALEZ, the defendant, lived -- and the address of the jail where she was detained in Mississippi, at the time she was detained there in connection with the attempt to fraudulently purchase a cellphone described above. Computer-1 also contained Google searches for "aeropuertas en Mississippi," which translates to "airports in Mississippi." In or around July 2017, Computer-1 also accessed the TD Bank page of "Joandra Tejada Gonzalez."

d. Computer-1 contained various indicators of involvement in the Fraud Ring, including:

i. Google searches for "casas vacias en Hazleton," which translates to "empty houses in Hazleton." Based on my participation in this investigation, I believe the purpose of this search was to locate empty homes to send and/or store fraudulently obtained cellphones and devices.

ii. Google and Google Chrome searches for "at&t my order status," "Verizon claim," "best buy check my upgrade," "instant checkmate" (which is a background checking website), "federal tax id number buy," "buy tax id number," "federal tax id number search," "driver license OH," and "driver license MO". Based on my participation in this investigation, I believe the purpose of these searches included purchasing victim PII, checking whether certain accounts with cellular service companies were entitled to a cellphone "upgrade" (one mechanism of the Fraud Ring), and checking the status of orders in furtherance of the scheme.

iii. The "top sites" on a web browser included "slilpp.ws" and "unicc.at".

1. Based on my training, experience, review of publicly available information, and conversations with other law enforcement officers, I am aware that Slilpp is essentially a marketplace of compromised accounts, which allows users to purchase customer login information, among other things; and unicc is primarily a marketplace for stolen credit card data.

2. Based on, among other things, my communications with a Cellphone Company-1 fraud investigator, I am aware that victim PII can be purchased on Slilpp for only \$3 to \$5.

iv. Google Chrome searches for "slip," "intelius," and "oscarbay," which are websites where victim PII can be purchased.

v. Evidence concerning the darkweb, including evidence that Computer-1 accessed the Tor Browser.

JOEL PENA

47. Based on, among other things, my review and analysis of documents and reports provided by Cellphone Company-1, I have learned the following about JOEL PENA, the defendant:

a. Between on or about July 5, 2015 and on or about July 8, 2015, PENA's name was used in connection with approximately ten compromised accounts of Cellphone Company-1 customers. Approximately 27 cellphones were fraudulently charged to these victimized accounts.

b. For approximately four of these compromised accounts, the billing address was also changed to a particular address in the Bronx associated with PENA based on, among other things, criminal history records (the "PENA Address").

c. This fraudulent activity, which appears to be attributable to PENA, has caused approximately \$25,264.98 in losses to Cellphone Company-1.

48. Based on, among other things, my review and analysis of documents and reports provided by Cellphone Company-2, I have learned the following about JOEL PENA, the defendant:

a. Between in or about 2014 and in or about 2016, PENA's name was used in connection with at least approximately 138 compromised accounts of Cellphone Company-2 customers in at least New York, New Jersey, Massachusetts, California, North Carolina, Pennsylvania, Tennessee, Texas, Maryland, Maine, Illinois, and Florida. Approximately 151 cellphones were fraudulently charged to these victimized accounts.

b. The billing addresses of approximately four Cellphone Company-2 customer accounts were changed to the PENA Address.

c. A variety of email addresses were associated with these compromised accounts, including:

- i. JOELPENA[four numbers]@gmail.com
- ii. JPENA[three numbers]@gmail.com
- iii. JPENA[four numbers]@gmail.com
- iv. JEILPENA[four numbers]@gmail.com
- v. JOELPENA[four numbers]@gmail.com
- vi. JMONEY[four numbers]@iCloud.com.

d. This fraudulent activity, which appears to be attributable to PENA, caused approximately \$101,980.65 in losses to Cellphone Company-2.

49. Based on conversations with CW-1, I have learned, among other things, the following:

a. JOEL PENA, the defendant, is a significant participant in the scheme.

b. PENA lives at the PENA Address.

c. Co-conspirator ("CC-2"), whom CW-1 named, works for PENA by fraudulently obtaining cellphones that were charged to compromised accounts.

d. To facilitate the fraud, PENA has worked with several co-defendants, including JHONATAN DIAZ, a/k/a "Nino," MARIO DIAZ, a/k/a "Memin," and RONNIE DE LEON. Specifically, PENA works under MARIO DIAZ. PENA's tasks include entering stores to fraudulently obtain phones through the unauthorized use of victims' social security numbers.

50. Based on my review and analysis of Western Union records, I have learned, among other things, the following:

a. Between on or about November 5, 2014 and on or about April 8, 2015, JOEL PENA, the defendant, sent approximately seven wire transfers -- totaling approximately \$13,500 -- to MARIO DIAZ, a/k/a "Memin," the defendant.

MARIO DIAZ, a/k/a "Memin"

51. Based on, among other things, my review of documents and reports provided by Cellphone Company-1, I have learned, among other things, the following about MARIO DIAZ, a/k/a "Memin," the defendant:

a. Between on or about July 7, 2015 and on or about July 8, 2015, MARIO DIAZ's name, or a derivative thereof, was used in connection with approximately two compromised Cellphone Company-1 accounts, which were used to fraudulently obtain approximately three cellphones.

b. This fraudulent activity, which appears to be attributable to MARIO DIAZ, has caused approximately \$2,747 in "upgrade" losses to Cellphone Company-1.

52. Based on, among other things, my review of documents and reports provided by Cellphone Company-2, I have learned the following about MARIO DIAZ, a/k/a "Memin," the defendant:

a. Between in or about 2012 and 2015, MARIO DIAZ's name was used in connection with at least approximately five compromised accounts of Cellphone Company-2 customers in at least New York, Florida, and California. At least approximately 18 cellphones were fraudulently charged to these victimized accounts.

b. Several email addresses were associated with these compromised accounts, including:

i. MARIODIAZ[three numbers]@gmail.com

ii. MARIODIAZ[five numbers]@Yahoo.com

c. Cellphone Company-2 suffered a loss of at least approximately \$9,673.05, which appears to be attributable to MARIO DIAZ.

53. Based on my review of records provided by Western Union, I have learned, among other things, the following:

a. Between on or about July 24, 2014 and on or about November 9, 2015, MARIO DIAZ, a/k/a "Memin," the defendant, sent five wire transfers totaling approximately \$4,860 to CC-3 (a suspected co-conspirator in the Dominican Republic whom I understand from CW-1 has been arrested by Dominican authorities).

b. Between on or about November 26, 2014 and on or about July 22, 2016, MARIO DIAZ sent four wire transfers totaling approximately \$8,100 to ISAAC CONCEPCION AQUINO, a/k/a "Kaka," the defendant. For three of these transfers, CONCEPCION's phone number, as reflected in the transfer records, had a Dominican Republic area code.

c. Based on my participation in this investigation, I believe that these transfers from MARIO DIAZ to CONCEPCION and CC-3 were payments for obtaining PII from the individuals in the Dominican Republic to be used to fraudulently obtain cellphones in the United States.

54. Based on conversations with CW-1, I have learned, among other things, the following:

a. JOEL PENA, the defendant, and CC-2 worked for MARIO DIAZ, a/k/a "Memin," in connection with the Fraud Ring.

b. MARIO DIAZ and ISAAC CONCEPCION AQUINO, a/k/a "Kaka," the defendant, used a black Audi ("Car-1").⁹

55. Based on my participation in this investigation, including the execution of the Warrant at the Mt. Vernon Residence, I have learned, among other things, that:

a. ISAAC CONCEPCION AQUINO, a/k/a "Kaka," the defendant, gave verbal consent to search Car-1.

b. Inside of Car-1 was a receipt, from on or about August 3, 2017, from a FedEx in Columbus, Ohio, for shipping materials.

c. Also inside of Car-1 was a receipt, from on or about July 25, 2017, for the issuance of an ID at the Bureau of Motor Vehicles in Youngstown, Ohio for \$8.50. The customer name on this receipt is a suspected co-conspirator ("CC-6").

⁹ Car-1 is not registered to MARIO DIAZ. It was registered to the brother of a co-conspirator in the Fraud Ring.

d. Based on my review of records provided by Cellphone Company-1, I know that, between on or about July 29 and August 5, 2017, CC-6's name was added to approximately 18 compromised accounts. For approximately 11 of these accounts, the billing address was changed to an address in Youngstown, Ohio.

56. Based on my participation in this investigation, the execution of the Warrant, as well as my conversations with others and my review of documents, reports, and photographs, I have learned the following, among other things:

a. MARIO DIAZ, a/k/a "Memin," the defendant, was present in the Mt. Vernon Residence, and his Dominican Republic Passport and identification card, Florida identification card, and United States Permanent Resident card were photographed.

b. Law enforcement officers observed Car-1 at the Mt. Vernon Residence on various occasions. For instance, on or about August 9, 2017, at approximately 1 p.m., I observed MARIO DIAZ exit the Mt. Vernon Residence, enter Car-1, and drive off.

c. MARIO DIAZ was found in a particular upstairs bedroom. In that bedroom, I found and seized, among other things, the following:

i. A receipt from Bank of America, dated June 27, 2017, indicating a deposit of \$2,000.

ii. A receipt from a Target store in the Bronx, in the amount of \$749.99 (the "Receipt"). The Receipt also listed a particular phone number, IMEI number, and SIM. On the back of the Receipt were handwritten notes with numbers -- which I believe to be dollar amounts associated with the Fraud Ring -- including "11,200," "Joel 2,520," and "Nino 2,520". Based on my training, experience, and participation in this investigation, I believe this handwritten note indicates that payment related to the Fraud Ring is either due to, or due from, JOEL PENA, the defendant, in the amount of \$2,520, and JHONATAN DIAZ, a/k/a "Nino," the defendant, also in the amount of \$2,520.

ISAAC CONCEPCION AQUINO, a/k/a "Kaka"

57. Based on my review and analysis of records from Cellphone Company-1, I have learned, among other things, the following:

a. The name of ISAAC CONCEPCION AQUINO, a/k/a "Kaka", or derivatives thereof, were used in connection with approximately two compromised Cellphone Company-1 accounts. Approximately three

cellphones were fraudulently obtained on these compromised accounts.

58. Based on my review and analysis of records prepared and provided by Western Union, I have learned, among other things, the following:

a. Between on or about February 23, 2014 and on or about June 8, 2015, ISAAC CONCEPCION AQUINO, a/k/a "Kaka," received 18 wire transfers totaling approximately \$22,327 from TOMAS GUILLEN, a/k/a "Diddy," the defendant. For 12 of these transfers, CONCEPCION's phone number, as reflected in the transfer records, had a Dominican Republic area code. Approximately 14 of 18 wire transfers list CONCEPCION AQUINO's known birthdate as the recipient's date of birth, based, among other things, on my review of photographs of his New York State Driver's License and U.S. Passport.

b. As noted above, between on or about November 26, 2014, and on or about July 22, 2016, CONCEPCION AQUINO received four wire transfers, totaling approximately \$8,100, from MARIO DIAZ, a/k/a "Memin," the defendant.

c. Between on or about May 13, 2015 and August 25, 2015, CONCEPCION AQUINO received two wire transfers of approximately \$4,500 from CW-1. For one of these transfers, CONCEPCION's phone number, as reflected in the transfer records, had a Dominican Republic area code.

d. Based on my participation in this investigation, and my conversations with CW-1, I believe that these transfers from GUILLEN, MARIO DIAZ, and CW-1 to CONCEPCION AQUINO were payments for obtaining PII from the individuals in the Dominican Republic to be used to fraudulently obtain cellphones in the United States.

59. Based on my conversations with CW-1, I have learned, among other things, the following:

a. ISAAC CONCEPCION AQUINO, a/k/a "Kaka," goes by the alias "Kaka." CW-1 has positively identified a photograph of CONCEPCION AQUINO.

b. Prior to coming to the United States, CONCEPCION AQUINO engaged in credit card fraud in the Dominican Republic and Puerto Rico.

c. TOMAS GUILLEN, a/k/a "Diddy," the defendant, introduced CW-1 to CONCEPCION AQUINO.

d. CW-1 described CONCEPCION AQUINO's role in the scheme as locating and infiltrating victim accounts on the computer, which PII he provides to others, including to GUILLEN.

e. In or about 2017, CONCEPCION AQUINO, GUILLEN, and JHONATAN DIAZ, a/k/a "Nino," the defendant, resided at the Mt. Vernon Residence.

f. As noted above, MARIO DIAZ, a/k/a "Memin," the defendant, and CONCEPCION AQUINO used Car-1.

60. Based on my participation in this investigation, the execution of the Warrant, as well as my conversations with others and my review of documents, reports, and photographs, I have learned the following, among other things:

a. During the execution of the Warrant, ISSAC CONCEPCION AQUINO, a/k/a "Kaka," the defendant, was found in a particular bedroom (the "CONCEPCION AQUINO Bedroom"), and his United States Passport, New York Driver License, and Dominican Republic identification card were photographed.

b. A computer was seized during the execution of the Warrant ("Computer-2") that is suspected to belong to and to have been used by CONCEPCION AQUINO.

c. Computer-2 contained evidence linking CONCEPCION AQUINO to the computer, including, but not limited to, the following:

i. Computer-2 contains Skype conversations with the username, Jeff012290, and display name "Jeff Bagwell." Based on my conversations with CW-1, my review of records and documents, and my review photos taken of CONCEPCION AQUINO's identifying documents, I believe this Skype account belongs to CONCEPCION AQUINO, in part because his New York State Driver's License and U.S. Passport show a date of birth of matching the number scheme in the Skype username, and CW-1 has indicated CONCEPCION AQUINO sometimes goes by the alias of "Jeff."

ii. IP address information, both local and public, indicate that this Skype user name, Jeff012290, repeatedly logged into the CONCEPCION AQUINO Computer.

d. Computer-2 contains the 15-minute long How-to Video, which, as noted above, details (in Spanish) the steps necessary to commit the cellphone fraud, including how to use victim PII to access victim accounts and order devices.

e. Inside of Car-1 was a receipt, from on or about August 3, 2017, from a FedEx in Columbus, Ohio, for shipping materials.

f. Also inside of Car-1 was a receipt, from on or about July 25, 2017, for the issuance of an ID at the Bureau of Motor Vehicles in Youngstown, Ohio for \$8.50. The customer name on this receipt is a suspected co-conspirator ("CC-6").

i. Based on my review of records provided by Cellphone Company-1, I know that, between on or about July 29 and August 5, 2017, CC-6's name was added to approximately 18 compromised accounts. For approximately 11 of these accounts, the billing address was changed to an address in Youngstown, Ohio.

g. Inside of the CONCEPCION AQUINO Bedroom was a MoneyGram receipt, dated July 29, 2017, where the "Sender" is identified as "Isaac Concepcion"; the recipient's expected location is "United States (OH)," which I believe to be Ohio; and the amount transferred is \$2,000.

h. Also inside of the CONCEPCION AQUINO Bedroom was a Wells Fargo Bank receipt, dated March 1, 2017, indicating a cash deposit of \$9,000.

i. Also inside of the CONCEPCION AQUINO Bedroom were two TD Bank Visa cards in the name of "Isaac David Concepcion"; a Capital One Quicksilver card in the name of "Isaac Concepcion"; and another card in the name of "Isaac Concepcion."

JHONATAN DIAZ, a/k/a "Nino"

61. Based on my conversations with CW-1, I have learned, among other things, the following:

a. JHONATAN DIAZ, a/k/a "Nino," the defendant, goes by the alias "Nino." CW-1 has positively identified a photograph of JHONATAN DIAZ.

b. JHONATAN DIAZ came to the United States on a fraudulent visa.

c. JHONATAN DIAZ has been an active participant in the Fraud Ring since at least in or about 2016 and continuing to the present. Among other roles, JHONATAN DIAZ obtains stolen PII from at least two co-conspirators in the Dominican Republic ("CC-4" and "CC-5"),¹⁰ recruits new individuals to participate in the Fraud Ring, and provides individuals with stolen PII with which to go into cellphone stores to fraudulently obtain cellphones.

d. At least in or about May 2017, JHONATAN DIAZ lived at the Mt. Vernon Residence, along with co-defendants TOMAS GUILLEN and ISAAC CONCEPCION AQUINO, a/k/a "Kaka," among others.

e. In or about June 2018, JHONATAN DIAZ was an especially active participant in the Fraud Ring, obtaining approximately 80 iPhones. During this time period, JHONATAN DIAZ and the Fraud Ring have been operating out of a particular apartment in the Bronx (the "Bronx Apartment"). On multiple occasions, MARIO DIAZ, a/k/a "Memín," the defendant, has gone to the Bronx Apartment to collect money from JHONATAN DIAZ, which I believe to be fraud proceeds.

f. JHONATAN DIAZ had previously been arrested in connection with this scheme.¹¹

¹⁰ Based on my review and analysis of records from Cellphone Company-2, I have learned, among other things, that between in or about January 2013 and in or about December 2013, the name of CC-4 was added to approximately three customer accounts of Cellphone Company-2. Each of these accounts were victims to fraudulent handset purchases. Approximately six cellphones were fraudulently obtained on these compromised accounts.

¹¹ Based on my review of a Montgomery County, Maryland police report, I have learned the following, among other things: On or about June 7, 2015, "Jhonatan Ernesto Diaz Azcona," whom I believe to be JHONATAN DIAZ, a/k/a "Nino," the defendant, and an individual with a Bronx address ("CC-8"), were both arrested in connection with CC-8's attempted fraudulent purchase of cellphones at an AT&T store in or around Bethesda, Maryland. CC-8 was attempting to obtain an "upgrade" phone and to use the Verizon Edge financing plan, pursuant to which the customer obtains the cellphone by initially paying only taxes (not the full price of the phone). The victim account holder was promptly contacted and affirmed that he did not authorize anyone to make any changes to his account. JHONATAN DIAZ had been inside of that same Apple store earlier that day. When interviewed by law enforcement in Maryland, JHONATAN DIAZ provided a Dominican Republic Passport and a

62. Based on my participation in this investigation, I know that "ninofiscò" is an Instagram account which features a public profile picture of an individual whom I believe to be JHONATAN DIAZ, a/k/a "Nino," the defendant.

63. Based on my participation in this investigation, the execution of the Warrant, as well as my conversations with others and my review of documents, reports, and photographs, I have learned the following, among other things:

a. JHONATAN DIAZ, a/k/a "Nino," the defendant, was present in the Mt. Vernon Residence when the Warrant was executed, and his Dominican Republic identification card was photographed.

b. A computer was seized during the execution of the Warrant ("Computer-3") that is suspected to belong to and to have been used by JHONATAN DIAZ.

c. Computer-3 contained evidence linking JHONATAN DIAZ to the computer, including, but not limited to, the following:

i. A Google Chrome login for "nino[four numbers]"; jump list data¹² with file paths ending in "nino" or "ninofisco[number]"; autofill data for ninofisco[four numbers]; Chrome browser web history to yhopmail.com,¹³ with "ninofisco[four numbers]" in the URL address; and a file on the desktop of Computer-3 named "Nino.txt"

d. Computer-3 contained various indicators of involvement in the Fraud Ring, including:

i. Chrome browser web history showing numerous visits to the websites att.com, including numerous URLs containing the phrase "upgrade phone," and bestbuy.com

fraudulent Dominican Republic Driver's License. He was found in possession of more than \$1,100 in United States currency and charged with conspiracy to commit theft and possession of a fraudulent government identification.

¹² Based on my review of publicly available information, a "jump list" is a feature that allows a computer user to view recently viewed documents.

¹³ Based on publicly available information, YOP mail provided free, disposable email addresses.

ii. Chrome browser web history and jump list data showing numerous visits to websites whose URLs include "intelius," "slilpp," "unicc.at," "robocheck," and "binlist".

1. Based on my training, experience, and involvement in this investigation, and review of publicly available information, I know that "intelius," "unicc.at," "slilpp," "robocheck," and "binlist" are darkweb and/or sites where victim PII, customer accounts, and/or credit card information can be purchased.

iii. A chat in which the two participants (neither of whose online names is Jhonatan Diaz) discuss thousands of dollars in payments using iTunes gift cards and Bitcoin. Based on my training, experience, and involvement in this investigation, I believe that these thousands of dollars of largely untraceable payments were likely for the purpose of purchasing victims' PII in furtherance of the fraud scheme.

64. Based on my review of documents provided by Western Union, I have learned the following, among other things, about JHONATAN DIAZ, a/k/a "Nino," the defendant:

a. Between on or about June 9, 2016 and on or about June 12, 2016, "Jhonatan Diaz," whom I believe to be JHONATAN DIAZ, the defendant, sent approximately four wire transfers to JOEL PENA, the defendant, totaling approximately \$3,174.

i. Based on my review of documents provided by Cellphone Company-1, I have learned, among other things, that on or about both June 18 and June 19, 2016, JOEL PENA fraudulently obtained a total of approximately four cellphones -- two in San Diego, California and two in North Escondido, California. Based on my training, experience, and involvement in this investigation, I believe that JHONATAN DIAZ's four payments to JOEL PENA in June 2016 were in connection with of JOEL PENA's four fraudulent cellphone purchases in June 2016.

b. In or about March 2013, "Jhonatan Diaz," whom I believe to be JHONATAN DIAZ, the defendant, sent approximately one wire transfer to TOMAS GUILLEN, a/k/a "Diddy," the defendant, for approximately \$299.99.

c. In or about June 2014, "Jhonatan Diaz," whom I believe to be defendant JHONATAN DIAZ, sent approximately one wire transfer to CC-4 for approximately \$482. The phone number provided by CC-4 has a Dominican Republic area code.

d. Between in or about November 2017 and in or about January 2018, "Jhonatan Diaz," whom I believe to be defendant JHONATAN DIAZ, sent approximately four wire transfers to CC-4, totaling approximately \$1,142. Each of the four wire transfers were sent to the Dominican Republic.

EDDY MORROBEL and RAYNIEL ROBLES

65. Based on my review and analysis of documents and reports prepared by Cellphone Company-1, I have learned, among other things, the following about EDDY MORROBEL, the defendant:

a. Between in or about February 2016 and in or about February 2017, MORROBEL's name, or derivatives thereof, were used in connection with approximately two compromised Cellphone Company-1 accounts. Approximately 13 cellphones were fraudulently obtained on these accounts. This fraudulent activity, which appears to be attributable to MORROBEL, caused approximately \$12,577 in losses to Cellphone Company-1.

b. The billing address on one compromised account was changed to an address in Miami, Florida, while the billing address on the other account was changed to an address in Spring Valley, New York. Both the Miami and Spring Valley addresses (along with additional addresses) are associated with MORROBEL in, among other things, New York City Police Department records.

c. Between in or about April 2017 and in or about May 2017, the name of "EDDY MORROBEL" was used in connection with two fraudulent accounts. Approximately 13 cellphones were fraudulently obtained on these accounts. For one of those two accounts, a particular email address, "EDDYGAME[four numbers]@Mail.com, is associated with compromising this account (in May 2017) from the IP Address associated with the Mt. Vernon Residence. Based on my training, experience, and participation in this investigation, including MORROBEL's presence in the Mt. Vernon Residence during the execution of the Warrant, I believe that MORROBEL had access to, and used, the EDDYGAME email address in furtherance of the fraud.

d. This fraudulent activity, which appears to be attributable to MORROBEL, caused approximately \$11,597.99 in losses to Cellphone Company-1.

66. Based on my review of Western Union records and documents, I have learned, among other things, that on or about November 24, 2014, "Eddy Morrobel," whom I believe to be EDDY MORROBEL, the defendant, sent a wire transfer of approximately

\$892 to "Isaac Concepcion Aquino," whom I believe to be ISAAC CONCEPCION AQUINO, a/k/a "Kaka," the defendant. The recipient's phone number is associated with the Dominican Republic, and the recipient's birthdate is CONCEPCION AQUINO's known birthdate. In addition, there are two more 2014 Western Union transfers -- each of which is more than \$800 but less than \$1,000 -- to "Isaac Concepcion Aquino" from an individual whose last name is "Morrobel," but whose first name is not Eddy.

67. Based on, among other things, my review and analysis of documents and devices seized during the execution of the Warrant at the Mt. Vernon Residence on or about August 15, 2017, as well as my participation in the execution of that warrant and my review of photographs, I have learned, among other things, the following:

a. During the execution of the Warrant, EDDY MORROBEL, the defendant, was present inside of the Mt. Vernon Residence, and his New York State Driver's License, U.S. Permanent Residence Card, Florida identity card, and work identification were photographed.

b. Several documents were seized from a particular room in which MORROBEL was believed to be staying, including two MoneyGram receipts in his name and handwritten notes with phone numbers, PINs, various dollar amounts (from \$300 to \$16,500), references to common Gigabyte sizes (e.g., "128," "256"), and references to types of cellphones (e.g., "S8 Plus," "S8 Regular").

c. A computer was seized during the execution of the Warrant ("Computer-4") that is suspected to belong to and to have been used by MORROBEL. Computer-4 contained various indicators of involvement in the Fraud Ring, including:

i. Google searches for "best buy upgrade," "best buy upgrade checker phone," "att activate phone," "att customer service," "verizon wireless oficinas centrales," "check my credit for verizon," "verizon.com check order status," "check my order status sprint," "sprint phone number," "most common last names for Spanish rich people," "liberar imei de verizon" (which translates to "release imei from Verizon"), "imei de verizon," "lycamobile contactos phone number," "lycamobile," "checkmate," "credit karma," "California driver license number format," "Utah driver license photo," "fedex customer service number," "fedex tracking," "chase routing numbers," and "add authorized user last name". Based on my experience and participation in this investigation, I believe the purpose of these searches included, among other things, obtaining information on unlocking phones, checking whether certain accounts were due an "upgrade" (one mechanism of the Fraud

Ring), and checking the status of orders with different cellphone providers, in furtherance of the scheme.

ii. Google searches for "intelius," "coinbase," "transunion," and "unicc."

1. Based on my training, experience, and involvement in this investigation, I know that "intelius" and "unicc" are darkweb sites where victim PII can be purchased.

2. Based on my training, experience, and involvement in this investigation, I know that Coinbase is an online marketplace that, among other things, operates Bitcoin exchanges. Coinbase therefore permits individuals to buy or sell Bitcoin using fiat currencies, including the U.S. Dollar.

iii. Browser history recommended words "slilipp" and "blockchain." Based on my training, experience, and involvement in this investigation, I know that the blockchain is widely used by cryptocurrencies including Bitcoin and contains transaction data.

iv. A Skype conversation containing a UPS Tracking Number.

v. An IP address associated with the Mt. Vernon Address.

vi. Various email addresses associated with Wiggio.com. Based on my training, experience, and participation in this investigation, I am aware that Wiggio mail was a free service that enabled group communication.

d. Computer-4 contained evidence linking MORROBEL to the computer, including, but not limited to, the following:

i. Several email addresses associated with MORROBEL, including the following:

- "Eddy Morrobel <chantellepirone@gmail.com>"
- "eddy morrobel <eddysocio@hotmail.com>"
- "Morrobeleddy@gmail.com"

- chantellepiron[two numbers]@gmail.com¹⁴

68. Based on my participation in this investigation, including the execution of the Warrant, I have learned, among other things, that a white Mercedes ("Car-2") was parked across the street from the Mt. Vernon Residence.

a. EDDY MORROBEL, the defendant, gave verbal consent to search Car-2, which is registered in the name of "Pura A. Piron," whom I believe to be a relative of his spouse.

b. Inside of Car-2, I found the following, among other things:

i. A handwritten note, which appeared to contain at least three phone numbers -- two associated with Cellphone Company-1 customers, one associated with a Cellphone Company-2 customer who resides in a nursing home.

ii. A receipt for a Bitcoin purchase on or about August 14, 2017.

iii. A receipt, dated August 11, 2017, from a transaction at Bank of America in the amount of \$400.

iv. A receipt, dated July 20, 2017, for a deposit at JPMorgan Chase Bank - Pelham Branch, in the amount of \$2,000.

v. A receipt, dated July 31, 2017, for a cash deposit at Capital One Bank, in the amount of \$1,500.

vi. A sales receipt, dated July 26, 2017, from a Speedcell Wireless MetroPCS in Akron, Ohio, for a Samsung Galaxy J3 cellphone associated with a particular phone number.

69. Based on my participation in this investigation, including the execution of the Warrant, I have learned, among other things, that two MoneyGram receipts were found in a particular bedroom in the Mt. Vernon Residence, and the "Sender" for each was "Eddy Morrobel," which I believe was EDDY MORROBEL, the defendant; the amount transferred in each case was \$1,000; the recipient's expected location for each monetary transfer is "United States (OH)," which I believe to be Ohio; and the dates for the transfer were June 14 and 29, 2017. Based on my training, experience, and

¹⁴ Based on information in a law enforcement database, I have learned, among other things, both that Chantelle Piron's spouse is named "Eddy" and that Eddy Morrobel's spouse's name is "Chantelle."

involvement in this investigation, I believe that MORROBEL was sending money to co-conspirators in furtherance of the Fraud Ring.

a. The recipient of the June 14, 2017 \$1,000 transfer from "Eddy Morrobel" was "Rayniel Robles," whom I believe to be RAYNIEL ROBLES, the defendant.

70. Based on my review of documents provided by Cellphone Company-1, I have learned, among other things, the following:

a. Between in or about June 2017 and in or about July 2017, ROBLES's name, or a derivative thereof (e.g., "Rayniel D. Robles"), was added as an authorized user to approximately 18 compromised accounts of Cellphone Company-1 customers. Approximately 58 cellphones were fraudulently obtained from these accounts. This fraudulent activity, which appears attributable to ROBLES, resulted in approximately \$50,339.42 worth of losses to Cellphone Company-1.

b. The period in which these accounts were compromised was same period during which EDDY MORROBEL, the defendant, paid ROBLES. In fact, between on or about June 9 and June 15, 2017, ROBLES fraudulently obtained approximately 26 cellphones in Ohio. On June 14, 2017, MORROBEL wired ROBLES \$1,000 in Ohio.

c. Of these approximately 58 fraudulently obtained cellphones, approximately two were obtained at stores in Kentucky, five in Pennsylvania, and 51 in Ohio.

d. For approximately 47 of these 58 compromised accounts, the "new billing address" was a particular address in Shaker Heights, Ohio which is listed as the address on "Rayniel Dario Robles"'s -- which I believe to be ROBLES's -- Ohio State Driver's License. Based on my training, experience, and involvement in this investigation, I believe that MORROBEL (from New York) was paying ROBLES (in Ohio) to fraudulently obtain cellphones in furtherance of the Fraud Ring.

71. Based on my review and analysis of documents and reports prepared by Cellphone Company-2, I have learned, among other things, the following about RAYNIEL ROBLES, the defendant:

a. Between on or about September 20, 2016 and on or about June 22, 2018, ROBLES's name, or derivatives thereof (e.g., "Rayneil Robles"), were used in connection with approximately 10 compromised accounts, that were used to fraudulently obtain approximately 19 cellphones.

b. This fraudulent activity, which appears to be attributable to ROBLES, caused approximately \$17,273.84 in losses to Cellphone Company-2.

RUDDY SANCHEZ

72. Based on my review and analysis of documents and reports prepared by Cellphone Company-1, I have learned, among other things, the following about RUDDY SANCHEZ, the defendant:

a. Between on or about May 24, 2015 and on or about August 4, 2015, SANCHEZ's name, or derivatives thereof, were used in connection with approximately 49 compromised Cellphone Company-1 accounts -- in California, Washington, Tennessee, and Colorado -- that were used to fraudulently obtain approximately 93 cellphones.

b. This fraudulent activity, which appears to be attributable to SANCHEZ, caused approximately \$84,481.75 in losses to Cellphone Company-1.

73. Based on my review and analysis of documents and reports prepared by Cellphone Company-2, I have learned, among other things, the following about RUDDY SANCHEZ, the defendant:

a. On or about October 31, 2014, and on or about March 18, 2017, SANCHEZ's name, or a derivative thereof (e.g., "Rudy Sanchez"), was linked to approximately two compromised Cellphone Company-2 accounts in California, which compromised accounts were used to fraudulently obtain approximately eight cellphones.

b. An email address is associated with one of these two compromised Cellphone Company-2 accounts -- rudysans@gmail.com -- which I believe to have been used by SANCHEZ.

c. This fraudulent activity, which appears to be attributable to SANCHEZ, caused approximately \$5,600 in losses to Cellphone Company-2.

74. Based on my review of MoneyGram records, I have learned the following, among other things:

a. On or about May 16, 2017, RUDDY SANCHEZ, the defendant, sent a wire transfer of approximately \$960 to "Ronnie Deleon," whom I believe to be RONNIE DE LEON, the defendant.

b. On approximately 15 occasions between on or about June 14, 2016 and on or about January 24, 2017, SANCHEZ sent wire

transfers to approximately three individuals in Hazleton, Pennsylvania (the "Three Recipients") -- the same city that JOANDRA TEJADA GONZALEZ, the defendant, has an address in (though these wire transfers were not addressed to her) -- totaling approximately \$10,418.

i. Based on my review of documents provided by the Glendale, California Police Department, I have learned, among other things, that two of the Three Recipients were arrested together, on or about November 9, 2017, for fraud, burglary, and grand theft, stemming from their fraudulent purchase (and attempted fraudulent purchase) of iPhones at Apple Stores in California; they were arrested in possession of new iPhones, cash, three Apple Store receipts, and a MoneyGram receipt. One of the Three Recipients was suspected of having engaged in the same fraud at other Apple stores in California during May and August of 2016. That individual waived her *Miranda* rights and admitted to local law enforcement, in substance and in part, and among other things, that she had tried to upgrade/finance an iPhone 8 Plus even though she had not met, and did not know, the actual account holder; she was supplied the last four digits of the pertinent Social Security Number by a man whom she met in New York; she was paid approximately \$500 per phone; and she consented to a search of her personal cellphone, which revealed several phone numbers followed by the word "good" as well as the text, "you can add or remove up to 10 authorized users." The other individual arrested that day also gave a confession in which she admitted, among other things, that she is paid \$100 per phone.

75. Based on my review of Western Union records, I have learned the following, among other things:

a. RUDDY SANCHEZ, the defendant, repeatedly sent wire transfers both to the Dominican Republic and to the Bronx, New York. One wire transfer that SANCHEZ sent was to an individual whose last name is "Morrobela," spelled the same way as EDDY MORROBEL, the defendant, but whose first name is not Eddy.

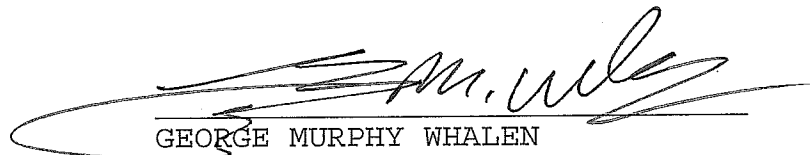
b. On or about April 19, 2017, SANCHEZ sent a wire transfer of approximately \$2,500, from the Bronx, New York, to a recipient ("CC-7") in San Bruno, California.

i. Based on my review of records provided by Cellphone Company-1, I have learned, among other things, that between on or about April 15 and August 8, 2017, CC-7's name (or a variant thereof) was added to approximately nine compromised accounts of Cellphone Company-1 customers, resulting in the

fraudulent purchase of approximately 34 cellphones -- each in California.

76. Based on my participation in this investigation, including my involvement in the execution of the Warrant at the Mt. Vernon Residence on or about August 15, 2017, I know that RUDDY SANCHEZ, the defendant, was present within the Mt. Vernon Residence that day and was photographed. I believe that SANCHEZ had access to, and used, Computer-3 because, among other things, CC-7's bank statement was present on that computer. As noted above, that computer contained wide-ranging evidence of involvement in the Fraud Ring, including, among other things, repeated browser searches for Robocheck and URLs involving "att," "resetPasscode," and "upgradephone".

WHEREFORE, the deponent respectfully requests that warrants be issued for the arrest of ISAAC CONCEPCION AQUINO, a/k/a "Kaka," MARIO DIAZ, a/k/a "Memin," TOMAS GUILLEN, a/k/a "Diddy," RONNIE DE LEON, JOSE ARGELIS DIAZ, JOEL PENA, JHONATAN DIAZ, a/k/a "Nino," EDDY MORROBEL, RUDDY SANCHEZ, MICHAEL ROQUE, RAYNIEL ROBLES, and JOANDRA TEJADA GONZALEZ, the defendants, and that they be arrested and imprisoned, or bailed, as the case may be.



GEORGE MURPHY WHALEN
Task Force Officer
U.S. Department of Homeland Security,
Homeland Security Investigations

Sworn to before me this
3rd day of August, 2018



THE HONORABLE BARBARA MOSES
United States Magistrate Judge
Southern District of New York