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

UNITED STATES OF AMERICA -v.- 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, Defendants.	**SEALED COMPLAINT** Violations of 18 U.S.C. §§ 1349, 1028A, and 2 COUNTY OF OFFENSE: BRONX 19MAG 6822

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).