2024R00804/DM/TAC

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	
	:	
v.	:	
	:	
DEMETRIO REYES MARTINEZ, a/k/a "CookieNerd,"	:	
ANDRICKSON JEREZ,	:	
EDICKSON LORA CASTILLO,	:	TO BE FILED UNDER SEAL
RAIMOND CABRERA DE LEON,	:	
LUIS MARTE TAVARES, a/k/a "Luis Marte Tavarez,"	:	Hon. Cathy L. Waldor
FREDERICK DUVERGE GUZMAN,	:	Mag. No. 25-9083
JULIO VAZQUEZ SANCHEZ, a/k/a "BotTrack,"	:	CRIMINAL COMPLAINT
ALEJANDRO THEN CASTILLO,	:	
WILSON PERALTA TAVAREZ,	:	
ECKER MONTERO HERNANDEZ,	:	
JEAN LUIS DIAZ DOMINGUEZ, a/k/a "Botija,"	:	
LUIS NUNEZ,	:	
JOEL SURIEL, a/k/a "La Melma,"	:	

I, Courtney Slaten, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement, Homeland Security Investigations, and that this Complaint is based on the following facts:

SEE ATTACHMENT B

Continued on the attached pages and made a part hereof.

Courtney Slaten

Courtney Slaten, Special Agent
Homeland Security Investigations

Special Agent Slaten attested to this Complaint by telephone pursuant to FRCP 4.1(b)(2)(A).

February 21, 2025 at
Newark, New Jersey

HONORABLE CATHY L. WALDOR
UNITED STATES MAGISTRATE JUDGE

Cathy L. Waldor (TAC)
Signature of Judicial Officer

Signed by Special Agent Slaten at Judge Waldor's direction pursuant to F.R.C.P. 4.1(b)(6)(C

ATTACHMENT A

COUNT ONE
(Conspiracy to Transport and Receive Stolen Property)

1. From in or around 2023, through the present, in Passaic County, in the District of New Jersey and elsewhere, the defendants,

DEMETRIO REYES MARTINEZ,
a/k/a "CookieNerd,"
ANDRICKSON JEREZ,
EDICKSON LORA CASTILLO,
RAIMOND CABRERA DE LEON,
LUIS MARTE TAVARES,
a/k/a "Luis Marte Tavarez,"
FREDERICK DUVERGE GUZMAN,
JULIO VAZQUEZ SANCHEZ,
a/k/a "BotTrack,"
ALEJANDRO THEN CASTILLO,
WILSON PERALTA TAVAREZ,
ECKER MONTERO HERNANDEZ,
JEAN LUIS DIAZ DOMINGUEZ,
a/k/a "Botija,"
LUIS NUNEZ,
JOEL SURIEL,
a/k/a "La Melma,"

did knowingly and intentionally conspire and agree with each other and with others to commit offenses against the United States, that is:

(a) to transport, transmit, and transfer in interstate and foreign commerce any goods, wares, merchandise, and money, of the value of $5,000 or more, knowing the same to have been stolen, converted, and taken by fraud, contrary to Title 18, United States Code, Section 2314; and

(b) to receive, possess, conceal, store, barter, sell and dispose of goods, wares, merchandise, and money of the value of $5,000 or more, which have crossed a State boundary after being stolen, and taken, knowing the same to have been stolen, unlawfully converted, and taken, contrary to Title 18, United States Code, Section 2315.

2. In furtherance of the conspiracy and in order to affect its objects, the defendants named herein committed and caused to be committed the overt acts set forth in Attachment B, in the District of New Jersey, and elsewhere.

In violation of Title 18, United States Code, Section 371.

COUNT TWO
(Conspiracy to Commit Wire Fraud)

1. **The Scheme to Defraud:** From in or around 2023 through on or about July 9, 2024, defendants **Alejandro Then Castillo** and **Wilson Peralta Tavarez** were employees of a mobile phone provider ("Victim-1") with a duty to refrain from seeking, accepting and agreeing to accept bribes and kickbacks in exchange for access to confidential Victim-1 records. From in or around 2023 through on or about July 9, 2024, defendants **Alejandro Then Castillo** and **Wilson Peralta** received money in exchange for confidential Victim-1 information, that is delivery information on Victim-1 customer orders of electronic devices.

2. From in or around 2023 through on or about July 9, 2024, in Passaic County, in the District of New Jersey, and elsewhere, the defendants,

ALEJANDRO THEN CASTILLO, and
WILSON PERALTA TAVAREZ,

did knowingly and intentionally conspire and agree with each other and with others to defraud Victim-1 of the right to the honest services of defendants **Alejandro Then** and **Wilson Peralta Tavarez** in the affairs of Victim-1, facilitated by the use of interstate wire transmissions, contrary to Title 18, United States Code, Sections 1343 and 1346.

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

COUNT THREE
(Transportation of Stolen Property)

Between on or about May 15, 2024 and on or about May 18, 2024, in Middlesex County, in the District of New Jersey, and elsewhere, the defendants,

ANDRICKSON JEREZ, and
ALEJANDRO THEN CASTILLO,

transported, caused to be transported, transmitted, and transferred in interstate and foreign commerce from New Jersey to New York any goods, wares, merchandise, and money, of the value of $5,000 or more, that is six iPhones, knowing the same to have been stolen, converted, and taken by fraud.

In violation of Title 18, United States Code, Sections 2314 and 2.

COUNT FOUR
(Transportation of Stolen Property)

On or about December 17, 2024, in the District of New Jersey, and elsewhere, the defendant,

EDICKSON LORA CASTILLO,

transported, caused to transport, transmitted, and transferred in interstate and foreign commerce from New Jersey to New York any goods, wares, merchandise, and money, of the value of $5,000 or more, that is five iPhones, an Apple Watch, an Air-tag with holder and strap, and a Samsung Galaxy phone, knowing the same to have been stolen, converted, and taken by fraud as a result of believing the official representation made by another person at the direction and with the approval of a Federal law enforcement officer that the property was robbed, stolen, converted, and taken.

In violation of Title 18, United States Code, Sections 2314, 21, and 2.

ATTACHMENT B

I, Courtney Slaten, am a Special Agent with Homeland Security Investigations ("HSI"). I am fully familiar with the facts set forth herein based on my own investigation, my conversations with witnesses and other law enforcement officers, and my review of reports, documents, and items of evidence. Where statements of others are related herein, they are related in substance and in part. Because this complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

I. Background

1. Law enforcement, including HSI, has been investigating an international network involved in the organized, widespread theft of electronic devices such as iPhones from FedEx and other shipping and logistics companies. As part of the scheme, certain co-conspirators (the "dispatchers") obtain tracking numbers and physical addresses associated with valuable shipments to be targeted for theft. The dispatchers offer this information for sale to other co-conspirators (the "runners") who will then wait for the packages at the delivery addresses and steal them. Stolen devices are brought to various "fence" locations, that is locations where the runners can sell the stolen devices. The stolen devices are then shipped overseas for sale and activation in other countries.

2. The dispatchers largely obtain the delivery information from two primary sources: (1) automated computer scripts; and (2) corrupt employees with access to data from companies such as Victim-1, a major U.S. cellular data provider.

3. Members of the conspiracy, including defendant **Demetrio Reyes Martinez, a/k/a "CookieNerd,"** ("**Reyes Martinez**"), developed and sold computer scripts or programs that scraped data from the customer tracking systems at FedEx and Victim-1. Until making changes to its package tracking system, FedEx limited the number of packages that could be tracked to 30 per query. Through the use of computer scripts, however, members of the conspiracy were able to get around this limitation to identify a large volume of FedEx packages that could be worth stealing (e.g. packages that contained multiple electronic devices).

4. Once such packages were identified, members of the conspiracy used Victim-1's customer tracking system to identify the devices being shipped, the destination city and state, and the name of the customer receiving shipment. By searching Victim-1's customer order system by FedEx tracking number, a Victim-1 customer name and city/state would, prior to Victim-1 system modifications, become available. Once the city/state and customer name were known, delivery addresses could be typically obtained by co-conspirators easily through online searches. Some

of the computer scripts themselves could be run to provide the full delivery address of Victim-1 orders. After both FedEx and Victim-1 implemented changes to their public and customer facing tracking systems, there was a substantial reduction in thefts of Victim-1 shipments from FedEx, with an apparent increase in theft from other delivery companies and mobile phone providers.

5. Co-Conspirators also identified packages for theft and obtained customer names and addresses through the use of corrupt Victim-1 employees, including defendants **Alejandro Then Castillo** ("**Then Castillo**") and **Wilson Peralta Tavarez** ("**Peralta Tavarez**"). Based on this investigation, **Then Castillo** and **Peralta Tavarez** worked together to provide co-conspirators with a large volume of Victim-1 shipment information in exchange for money.

6. The investigation has revealed that through this scheme, thousands of packages have been stolen from customers, resulting in millions of dollars in loss to FedEx, Victim-1, and other victims.

II. Defendants and Roles

7. **Reyes Martinez** is a citizen and resident of the Dominican Republic. Operating under his online persona "CookieNerd," **Reyes Martinez** created, operated and sold various computer scripts used in this scheme and other criminal activity.

8. Defendant **Andrickson Jerez** ("**Jerez**") ran a fence location out of a residential building at 2227 University Avenue, Bronx, NY ("2227 University") where stolen devices were purchased from runners.

9. Defendant **Edickson Lora Castillo** ("**Lora Castillo**") was a dispatcher who provided runners with delivery addresses to target for theft.

10. Defendant **Raimond Cabrera De Leon** ("**Cabrera De Leon**") and **Luis Marte Tavares** ("**Marte Tavares**") helped run the fence location at 2227 University on a daily basis. **Cabrera De Leon** was a co-owner of 2227 University.

11. Defendant **Frederick Duverge Guzman** ("**Duverge Guzman**") was a dispatcher who sold delivery addresses to runners. **Duverge Guzman** also directed runners to fence locations, including 2227 University, to sell the stolen devices.

12. **Then Castillo** was an employee of Victim-1 at a Victim-1 store in Paterson, NJ from in or around 2018 through on or about July 9, 2024. **Then Castillo** received payments for his unauthorized disclosure of Victim-1 customer tracking data. According to an investigation conducted by Victim-1, **Then Castillo** used his Victim-1 login credentials to track approximately 358 Victim-1 shipments that were subsequently stolen in transit. According to Victim-1, **Then Castillo** had

no legitimate reason to access the Victim-1 order tracking system at this volume in the ordinary course of his employment.

13. **Peralta Tavarez** was a manager at a Victim-1 store in Fort Lee, New Jersey. **Peralta Tavarez** assisted **Then Castillo** by providing additional Victim-1 customer order tracking data to **Then Castillo**.

14. Defendant **Julio Vasquez Sanchez, a/k/a "BotTrack,"** ("**Vasquez Sanchez**") was a dispatcher who sold tracking and delivery address information to runners for theft. **Vasquez Sanchez** ran a "channel" on an encrypted messaging application Telegram where he offered customer tracking and address information for sale.

15. Defendant **Joel Suriel, a/k/a "La Melma,"** ("**Suriel**") was the owner of Wyckoff Wireless at 309 Wyckoff Avenue, Brooklyn, NY ("309 Wyckoff") where he operated a fence location where he and his employees purchased stolen devices. On or about November 5, 2018, in the District of Kansas, **Suriel** pled guilty to wire fraud conspiracy in United States v. Joel Suriel, a/k/a "La Melma," et al. According to documents filed in this case, **Suriel** admitted to his role in a scheme targeting Victim-1 where stolen Victim-1 customer identities were used to fraudulently acquire cell phones from Victim-1. **Suriel's** role in that case was purchasing these fraudulently obtained iPhones at his store, 309 Wyckoff. Specifically, on or about July 19, 2017, an undercover law enforcement officer sold five fraudulently obtained iPhones to **Suriel** at 309 Wyckoff. On or about November 3, 2023, **Suriel** was re-sentenced to 6 months' imprisonment and one year of supervised release. He is currently on supervised release.

16. Defendants **Ecker Montero Hernandez** ("**Montero Hernandez**"), **Luis Nunez** ("**Nunez**"), and **Jean Luis Diaz Dominguez** ("**Diaz Dominguez**") were runners who worked together as a crew stealing packages in New Jersey and around the country. They frequently traveled, using short-term vacation rentals and hotels as a base of operations to target new areas for theft. They frequently shipped their stolen devices in bulk shipments to **Suriel** at 309 Wyckoff.

III. Reyes Martinez and the Computer Scripts

17. During the course of the investigation, law enforcement identified an online persona "CookieNerd" as a broker of computer scripts used to obtain tracking and address data from FedEx, Victim-1, and other victims being targeted for theft. A review of a cell phone seized from a member of the conspiracy ("Co-Conspirator-1") revealed that Co-Conspirator-1 sent a screenshot via an encrypted messaging application to "CookieNerd" documenting a payment Co-Conspirator-1 made for the purchase of a computer script. The screenshot showed further that the bank account that received the payment was held in **Reyes Martinez**'s true name, "Demetrio Reyes." Further, as set forth below, law enforcement engaged in an undercover

purchase of computer scripts from "CookieNerd." An analysis of one these scripts showed that it ran, in part, by connecting to servers hosted at a U.S. provider, which was subscribed to by **Reyes Martinez** in his true name "Demetrio Reyes." Finally, law enforcement showed a photograph of **Reyes Martinez** to a person who knows the individual using the online persona "CookieNerd," and this person confirmed that **Reyes Martinez** is, in fact, the individual he or she knows to be "CookieNerd." Based on this information and additional evidence gathered through this investigation, there is probable cause to believe that **Reyes Martinez** is "CookieNerd".

18. Law enforcement review of Co-Conspirator-1's phone revealed that **Reyes Martinez** sold a FedEx tracking script to Co-Conspirator-1 and then helped Co-Conspirator-1 use the script. For example, on or about August 19, 2023, Co-Conspirator-1 sent **Reyes Martinez** a video clip of a computer file named "FedEx TR." **Reyes Martinez** responded with instructions on how to run the program.

19. On or about October 19, 2024, a law enforcement officer ("UC1") using an undercover computer, contacted **Reyes Martinez**, using the CookieNerd handle, on the encrypted messaging service Telegram. In Spanish, UC1 negotiated a price of $450 in Bitcoin in exchange for the sale, installation, and configuration of a programming script designed to automate the random querying of sequential numbers on FedEx's tracking website to obtain the following information: city and state of origin, and city and state of destination. After making payment in Bitcoin, UC1 received from **Reyes Martinez** three links at a file hosting company to download the script. The three links downloaded three executable application files: (1) a licensing application; (2) "fedexTR.exe"; and (3) "lookup-fedex2.exe."

20. On or about October 22, 2024, while UC1 was in New Jersey, UC1 granted **Reyes Martinez** remote access to an undercover computer. **Reyes Martinez** accessed a list of proxy servers (servers used to hide the true internet-protocol address and identity of a computer) from the undercover computer. **Reyes Martinez** explained to UC1 how to use the FedEx executable files to find valid tracking numbers. UC1 also asked **Reyes Martinez** about the purchase of a script for Victim-1 orders and **Reyes Martinez** said the price for that script was $750.

21. Subsequently, law enforcement ran the FedEx tracking script purchased from **Reyes Martinez** and used it to generate valid tracking numbers that could then be run against Victim-1's customer order system to identify valuable Victim-1 shipments to steal.

22. On or about November 4, 2024, UC1 and **Reyes Martinez** texted via the Telegram encrypted chat application regarding the potential purchase of a Victim-1 script. **Reyes Martinez** stated that Victim-1 updated its system, and the Victim-1 script no longer worked. **Reyes Martinez** sent UC1 a screenshot of the customer facing order tracking system for Victim-1. The system required that the customer enter a last name that was used for the order, thus showing that the

Victim-1 customer system would no longer reveal full names of customers. Following this screenshot, **Reyes Martinez** stated in substance in Spanish that "now they are asking you for a last name. . .these guys are exhausting [Victim-1] with all the thefts of tracking lol."

23. On or about December 16, 2024, a forensic analysis on the FedEx script showed that **Reyes Martinez** configured it to connect to a server in his own name prior to tracking any FedEx packages. This was part of a licensing verification system that **Reyes Martinez** used to prevent unauthorized users from copying and running the script without payment. The analysis also showed that the script used proxies to query FedEx servers in an effort to get around FedEx data limits.

24. On or about January 22, 2025, UC1 purchased a script for another shipping company from **Reyes Martinez**. After UC1 paid the agreed price of $500 in Bitcoin, **Reyes Martinez** installed the program remotely on the undercover computers. This script worked similar to the FedEx script described above.

IV. Corrupt Victim-1 Employees Then Castillo and Peralta Tavarez Provide Customer Tracking Information

25. **Then Castillo** was a Victim-1 employee who worked as a retail sales associate at a Victim-1 store in Paterson. According to Victim-1 representatives, **Then Castillo** and another employee ("Employee-1") came under suspicion because their credentials were used to search an excessive number of electronic device orders. These queries searched by tracking number and exposed details of Victim-1 shipments of devices, including customer name, address, and the types of electronic devices purchased.

26. According to Victim-1 records, between on or about February 21, 2024, and on or about May 16, 2024, **Then Castillo**'s login credentials were used to conduct 1,169 queries in Victim-1's order tracking system. These queries were followed by the in-transit theft of 358 Victim-1 shipments, valued at $574,414.02. A review of store security video footage for a sample of these orders confirmed that **Then Castillo** accessed the order tracking system for no apparent business purpose.

27. According to Victim-1 records, between on or about March 2, 2024, and on or about May 20, 2024, Employee-1's login credentials were used to conduct 952 queries in the order tracking system. These queries were followed by the in-transit theft of 223 Victim-1 shipments, valued at $77,297.23. Victim-1 security reviewed store surveillance video of a sampling of five queries attributed to Employee-1's login credentials. The surveillance video revealed that **Then Castillo** was responsible for accessing the system using Employee-1's login credentials and taking pictures of a Victim-1 tablet screen with his phone. For example, records show that Employee-1's credentials were used on May 16, 2024, between 6:14-6:18 p.m. Surveillance video showed that, during this time period, **Then Castillo** was sitting in the store

breakroom in possession of a tablet and cell phone. **Then Castillo** used his cell phone to take a picture of the tablet screen.

28. Employee-1 was interviewed by Victim-1 security personnel on July 10, 2024. He denied sharing his credentials with **Then Castillo** and did not know how his credentials were compromised. Employee-1 stated that he did not recall ever using order tracking system and was not familiar with it.

29. According to one of **Then Castillo**'s supervisors at Victim-1, on or about July 9, 2024, the same day that Victim-1 security personnel had been conducting interviews at other Victim-1 locations, **Then Castillo** ran out the store, never returned, and submitted his resignation by email.

30. According to Victim-1 records, the login credentials for an employee at a Victim-1 store in Fort Lee, New Jersey ("Employee-2") conducted approximately 400 searches on the Victim-1 order tracking system between on or about May 9, 2024, and on or about May 21, 2024. These queries were followed by the in-transit theft of approximately 35 orders consisting of 67 devices, with a value of $63,879.34. A review of store surveillance video at the Fort Lee location of five randomly selected queries revealed that Employee-2 was not using the order tracking system during the times the queries were conducted. On one of these occasions, Employee-2's store manager **Peralta Tavarez** could be seen on video using a Victim-1 tablet at the time of the query. Employee-2 told Victim-1 security personnel that he did not use his login credentials to conduct the queries. Employee-2 also stated that he did not know about the order tracking system until a customer came to the store in or around May 2024 and asked about the status of a shipment. According to Employee-2, **Peralta Tavarez** then showed him how to use the system. Employee-2 also stated that **Peralta Tavarez** once asked Employee-2 for his login credentials, but Employee-2 declined to provide them.

31. On or about January 9, 2025, **Then Castillo** arrived at Newark Liberty International Airport, returning from a trip to the Dominican Republic. U.S. Customs and Border Protection ("CBP") conducted a routine interview of **Then Castillo** who consented to a search of his iPhone (the "**Then Castillo** Phone"). A preliminary, manual search of the **Then Castillo** Phone revealed communications on an encrypted messaging application where **Then Castillo** was providing others with images from Victim-1's order tracking system. HSI made a copy of the data on **Then Castillo's** Phone.

32. A subsequent court authorized search of the **Then Castillo** Phone revealed that **Then Castillo** communicated regularly with **Peralta Tavares**, using a phone subscribed to in his own name. These communications show that **Then Castillo** and **Peralta Tavares** worked together to share order tracking information, received money for their work, and recruited other Victim-1 employees into the scheme. Specifically, a review of the Then Castillo Phone revealed that **Then**

Castillo and **Peralta Tavares** exchanged approximately 365 images of Victim-1 orders from the order tracking system, which included customer names and addresses as well as tracking numbers.

33. Further, on or about May 15, 2024, **Then Castillo** forwarded **Peralta Tavares** a voice recording, in Spanish. The recording appears to be a message **Then Castillo** received from individuals paying him. The message stated in substance, "Look boss, that is something for sure even if we do not make anything, we still pay you. Because your work is that, you send the photo and look, he gave you his word and after next week, I will settle with him because this week we had to buy a program. We going to give you the $2,000 you want. You understand, so you can put another person to help you. And it depends, even $2,500. Because you understand, because it suits us for you to be active." Based on this investigation, law enforcement believes that the message reflects that **Then Castillo** was receiving $2,000 (which could be increased to $2,500) if he recruited another Victim-1 employee.

34. A review of data from the **Then Castillo** Phone further showed that **Then Castillo** was in contact with another co-conspirator ("Co-Conspirator-2") who received Victim-1 order tracking information from **Then Castillo**. Between on or about May 15, 2024, and on or about May 24, 2024, Co-Conspirator-2 forwarded hundreds of FedEx tracking numbers to **Then Castillo**, who, in turn provided Co-Conspirator-2 with approximately 305 images that appear to be photos displaying Victim-1's order tracking system, including customer names and addresses.

35. One such order sent from **Then Castillo** to Co-Conspirator-2 was a May 15, 2024, order by a Victim-1 customer in Iselin, New Jersey, who ordered six iPhones from Victim-1 (the "Iselin Order"). The six iPhones were valued at more than $5,000. The Iselin Order, including the FedEx tracking number, customer name, and physical address were displayed in an image that appears to be a photo of the Iselin order on a Victim-1 store tablet, which is a device **Then Castillo** used in the course of his employment. According to Victim-1 login records, on May 16, 2024, **Then Castillo** accessed the Victim-1 order tracking system and searched the FedEx tracking number for the Iselin Order. The Iselin Order customer later reported to Victim-1 that the Iselin Order was stolen and never received.

36. On or about May 18, 2024, New York Police Department ("NYPD") officers observed a sports utility vehicle running and double parked on West 42nd Street in Manhattan blocking traffic and a bus lane. As they approached the vehicle, **Jerez** and several individuals walked away and crossed the street. The vehicle was left unlocked and running, with no driver, passenger or any person claiming ownership. Inside the vehicle, officers found approximately 72 new, unopened iPhones, multiple other electronic devices, approximately $5,972 cash, credit cards with different names and several apparently forged driver's licenses with different names and photos. During the search, **Jerez** returned to the vehicle and said that it was his vehicle. **Jerez** was arrested for possession of forged identity documents.

37. An inspection of the serial numbers on the iPhones found in **Jerez's** Jeep was conducted. Amongst the iPhones recovered were the six specific iPhones that were shipped by Victim-1 via FedEx and subsequently stolen as part of the Iselin Order.

38. According to Victim-1 representatives, the Victim-1 order tracking system is hosted on computer servers located outside the state of New Jersey.

V. Jerez, Lora Castillo, and the 2227 University Operation

39. In the summer of 2024, a runner ("Runner-1") was arrested while trying to steal a FedEx package in New York. A subsequent search of Runner-1's phone revealed that **Jerez**, using an encrypted messaging application with a phone number that **Jerez** had previously provided to NYPD when interviewed (the "**Jerez** Phone"), instructed Runner-1 to bring stolen devices to different locations, including 2227 University. On or about June 27, 2024, **Jerez** sent an image of 2227 University from a publicly available website to Runner-1. On or about June 25, 2024, Runner-1 sent an image to **Jerez** from a peer-to-peer payment application stating "payment from Andy." Based on this investigation, **Jerez** sometimes goes by the name Andy, which is short for his first name, Andrickson. Further, Runner-1 listed "Andy" as the name for the **Jerez** Phone in Runner-1's contact list.

40. In or around October 2024, an individual cooperating with law enforcement ("CW1") received an address and tracking number for a FedEx delivery in Staten Island from **Lora Castillo** via an encrypted messaging application. **Lora Castillo** was using an encrypted messaging account that was assigned a phone number ("**Lora Castillo** Phone-1"). **Lora Castillo** communicated with CW1 via a video chat using the encrypted messaging application and **Lora Castillo**'s face was visible. **Lora Castillo** instructed CW1 to go to the address, wait for the FedEx delivery of an Apple iPhone, and to steal the package once it was delivered. CW1 went to the address and sent **Lora Castillo** a picture to confirm CW1 was there. CW1 did not steal this package. Once FedEx made the delivery, CW1 stated to **Lora Castillo** that CW1 had stolen the package when, in fact, law enforcement had provided CW1 with a different new iPhone.

41. **Lora Castillo** then instructed CW1 to go to another address in Staten Island on or about the same day to steal another package. CW1 went to this second address, took a photo, and sent it to **Lora Castillo**. Following law enforcement instructions, CW1 then told **Lora Castillo** that CW1 was unable to steal the second package.

42. At approximately 4 p.m. on or about the same day, CW1 called **Lora Castillo** to ask where CW1 should bring the "stolen" iPhone from Staten Island. **Lora Castillo** instructed CW1 to go to 2227 University Avenue to sell it.

43. 2227 University is a two-story house, which, according to public records, is a single-family house. However, it appears that there are multiple tenants, and the building may be operating as a multi-unit apartment or single-room occupancy complex. Co-conspirators use a small, fortified "store" for the activity being conducted at 2227 University. The "store" appears to be a makeshift room, likely built through illegal or unpermitted construction, on the front porch that connects to a first-floor residential area or apartment. The "store" contains a tinted window with a drawer underneath where individuals place stolen devices and receive payment, without seeing the person receiving the stolen devices or making the payment.

44. At approximately 6:45 p.m. on or about the same day, while under surveillance, CW1 entered 2227 University Avenue while wearing a recording device and sold the iPhone that was provided by law enforcement. CW1 received $440 in cash for the iPhone. According to CW1, and subsequently corroborated by a review of the recording, at 2227 University Avenue, CW1 entered a tiny fortified "store" with armed security, which in fact was a makeshift room attached to what appears to be a first-floor residential apartment. CW1 described a tinted window and a drawer under the window which was used to deliver the stolen phone and receive payment. CW1 stated that CW1 was able to observe through the tinted window a large quantity of phones, cash, and a firearm.

45. On or about December 17, 2024, CW1 received a list of FedEx tracking numbers from **Lora Castillo** for theft. CW1 selected eight shipments to various towns in New Jersey from this list. Law enforcement contacted FedEx regarding these shipments, and FedEx agreed to allow law enforcement to "steal" these packages as part of this investigation. With FedEx's assistance, law enforcement met with the delivery driver assigned to deliver each of the eight shipments and obtained the packages prior to delivery to the customers.

46. The packages were opened by law enforcement and photographed. CW1 sent the photographs to **Lora Castillo**. The packages in total contained five iPhones, an Apple Watch, an Air-tag with holder and strap, and a Samsung Galaxy phone. In total, these devices were valued at over $5,000. **Lora Castillo** instructed CW1 to bring the items to an address on South Street, New York, New York. Law enforcement placed the devices inside a red and beige bag bearing the logo for a big-box store (the "Store Bag") and gave the Store Bag to CW1 for delivery to **Lora Castillo**. At approximately 8:45 p.m., law enforcement observed as CW1 met with **Lora Castillo**, who arrived in a black sedan (the "**Lora Castillo** Vehicle"). CW1 exited CW1's vehicle and entered the **Lora Castillo** Vehicle at the corner of South Street and Clinton Street. During a recorded conversation, CW1 delivered the Store Bag of devices to **Lora Castillo**. **Lora Castillo** paid CW1 $1,300 in cash for the devices plus an additional $100 tip.

47. During the investigation, law enforcement has monitored a pole camera which records activity at 2227 University. A review of this video shows that 2227 University receives a constant stream of traffic with individuals bringing in bags appearing to contain iPhones and other electronic devices and exiting a short time later without the bags. The conduct is so open that sometimes the individual runners will openly carry the boxes with the devices into 2227 University and return without the devices.

48. Review of the pole camera also shows that **Cabrera De Leon** and **Marte Tavares** work at 2227 University on a daily basis. There is so much business traffic that large black garbage bags filled with what appears to be electronic devices are brought out of 2227 University multiple times a day, usually at least five times, sometimes as many as a dozen times. The bags are brought to another location in the Bronx, typically by **Cabrera De Leon**.

49. For example, review of the 2227 University pole camera footage revealed that on or about December 8, 2024, two males entered 2227 University at approximately 1:40 p.m. carrying what appeared to be small cellphone boxes. They later exited 2227 University without these boxes. At approximately 2:30 p.m., another male entered 2227 University with a bag and then exited a short time later with no bag. At approximately 4:50 p.m., **Jerez** parked in the driveway of 2227 University driving a blue sports utility vehicle ("the **Jerez** Vehicle"). After approximately 15-20 minutes, **Jerez** exited 2227 University with an unknown male. The unknown male was carrying a large black plastic bag, which he then placed inside the **Jerez** Vehicle. **Jerez** then departed. At approximately 5:45 p.m., **Jerez** returned to 2227 University in the **Jerez** Vehicle and entered the building. At approximately 6:05 p.m., **Jerez** exited 2227 University holding multiple large bags and placed them inside the **Jerez** Vehicle.

50. Review of the video further revealed that on or about December 16, 2024, at approximately 7:45 p.m., a different make and model of blue sports utility vehicle (the "**Marte Tavares** Vehicle") was parked near 2227 University and a white transport van with Pennsylvania plates (the "**Cabrera De Leon** Vehicle") was parked in the driveway.[1] At approximately 7:49 p.m., **Marte Tavares** and **Cabrera De Leon** exited 2227 University. **Cabrera De Leon** was carrying a large black plastic bag as **Marte Tavares** opened trunk of the **Marte Tavares Vehicle** and **Cabrera De Leon** placed the bag inside. **Marte Tavares** drove away while

[1] As set forth in part V below, this same day, December 16, 2024, at approximately 6:17 p.m., surveillance video captured **Marte Tavares** entering Wyckoff Wireless at 309 Wyckoff Ave, Brooklyn, NY carrying a large blue paper bag and a large black plastic bag and delivering them to an employee. At approximately 6:28 p.m., **Suriel** was observed exiting 309 Wyckoff carrying what appears to be the same blue paper bag delivered by **Marte Tavares.**

Cabrera De Leon returned to 2227 University. At approximately 7:55 p.m. **Cabrera De Leon** exited 2227 University carrying multiple bags. At approximately 8:00 p.m., the **Cabrera De Leon** Vehicle backed out of the driveway and departed.

51. Later, at approximately 8:32 p.m., the **Marte Tavares** vehicle returned to 2227 University and **Marte Tavares** entered the building. At approximately 8:44 p.m., the **Cabrera De Leon** Vehicle returned to 2227 University. At approximately 8:57 p.m., **Marte Tavares** exited 2227 University carrying a large black plastic bag. **Marte Tavares** opened the trunk of the **Cabrera De Leon** Vehicle and placed the bag inside. The **Cabrera De Leon** Vehicle then departed.

52. According to the video surveillance, on or about December 20, 2024, **Jerez** arrived at 2227 University driving the **Jerez** Vehicle at approximately 5:34 p.m. At approximately 5:36 p.m., **Marte Tavares**, exited 2227 University carrying two large black plastic bags, which he placed inside the **Jerez** Vehicle. **Jerez** then departed in the **Jerez** Vehicle.

53. The pole camera footage further shows that on or about December 21, 2024, at approximately 4:01 p.m., an unknown male entered 2227 University holding two small white boxes that appeared to contain Apple products, possibly an Apple Watch and Apple tablet. This unknown male exited 2227 University a short time later without these boxes in hand. At approximately 3:37 p.m., the **Lora Castillo** Vehicle double parked in front of 2227 University. **Lora Castillo** exited the **Lora Castillo** Vehicle and entered 2227 University. At approximately 5:01 p.m., the **Marte Tavares** Vehicle was parked in the driveway of 2227 University. At approximately 6:30 p.m., **Marte Tavares** exited 2227 University carrying a large plastic bag. **Marte Tavares** placed the bag in the trunk of the **Marte Tavares** Vehicle and drove away. At approximately 7:27 p.m., the **Marte Tavares** Vehicle returned to 2227 University and **Marte Tavares** entered the building.

54. According to the video surveillance, on or about December 25, 2024, at approximately 3:34 p.m., a male entered 2227 University carrying a large white bag which appeared to be an Apple bag. The male departed 2227 University at approximately 3:37 p.m. without the bag. At approximately 3:44 p.m., **Cabrera De Leon**, carrying this white Apple bag and a large black plastic bag, exited 2227 University. **Cabrera De Leon** placed both bags in the back of the **Cabrera De Leon** Vehicle, which was parked in the driveway, and drove away.

55. According to the video surveillance, on or about December 26, 2024 at approximately 7:30 p.m. **Cabrera De Leon**, driving the **Cabrera De Leon** Vehicle, parked in the driveway of 2227 University and entered. At approximately 7:35 p.m., **Cabrera De Leon** exited 2227 University carrying a large plastic bag, which he placed in the back of the **Cabrera De Leon** Vehicle. He then drove away. At approximately 9:29 p.m., **Cabrera De Leon** returned to 2227 University and parked

the **Cabrera De Leon** Vehicle in the driveway. At 9:38 p.m., **Cabrera De Leon** exited 2227 University carrying a large plastic bag, which he placed in the back of the **Cabrera De Leon** Vehicle, before departing. Law enforcement followed the **Cabrera De Leon** Vehicle. **Cabrera De Leon** appeared to be engaged in counter surveillance techniques during this time by making sudden stops and changing speeds.

56. According to the video surveillance, on or about December 27, 2024, at approximately 11:31 a.m., an unknown male was observed exiting a white luxury vehicle with Pennsylvania plates and entering 2227 University. He entered and exited 2227 University several times before retrieving a white bag from another vehicle at approximately 11:49 a.m. He then re-entered the white luxury vehicle parked in front of 2227 University. At approximately 12:02 p.m., **Cabrera De Leon** drove the **Cabrera De Leon** Vehicle to 2227 University and parked in the driveway before entering the building. The unidentified male from the white luxury vehicle exited his vehicle and met with **Cabrera De Leon** on the steps of 2227 University. The unidentified male retrieved an item from his white luxury vehicle and gave it to **Cabrera De Leon** before entering 2227 University.

57. On December 27, 2024, at approximately 12:49 p.m., **Lora Castillo** exited the **Lora Castillo** Vehicle and entered 2227 University carrying a plastic bag. At approximately 1:01 p.m., **Lora Castillo** exited 2227 University without the bag. He departed in the **Lora Castillo** Vehicle. According to CW1, **Lora Castillo** was delivering Samsung Galaxy phones and iPhones to 2227 University. According to CW1, **Lora Castillo** stated that these devices were stolen from Ozone Park. Also on December 27, 2024, **Lora Castillo** posted a "story" to his personal account on social media. The "story" contained a photo of 3 Samsung Galaxy phones and 2 iPhones in their boxes resting on the seat of a vehicle.

58. According to the video surveillance, on or about December 28, 2024, at approximately 7:46 p.m., the **Jerez** Vehicle parked in front of 2227 University. At approximately 7:48 p.m., a male exited 2227 University carrying two large black plastic bags, which he placed inside the **Jerez** Vehicle with the assistance of a person known to this investigation as a co-owner of 2227 University.

59. On or about January 12, 2025, law enforcement observed **Cabrera De Leon** arrive at 2227 University in the **Cabrera De Leon** Vehicle. He entered 2227 University and exited seven minutes later carrying two black bags. Law enforcement was able to observe one white box sticking out of one of the bags, which appeared to be a box for an Apple laptop or tablet. **Cabrera De Leon** placed the black bags in the back of the **Cabrera De Leon** Vehicle and drove away. Law enforcement observed **Lora Castillo** drive the **Lora Castillo** Vehicle to 2227 University at approximately 3:00 p.m. He parked in front of 2227 and exited the **Lora Castillo** Vehicle carrying a white box that appeared to be an iPhone box and entered 2227

University. Approximately 10 minutes later, he exited 2227 University without the iPhone box. **Lora Castillo** then departed in the **Lora Castillo** Vehicle.

60. Through surveillance and the monitoring of pole cameras, law enforcement has observed that the Co-Conspirators, most frequently **Cabrera De Leon**, transport multiple shipments of electronic devices in large plastic bags multiple times a day. They are brought from 2227 University to a residential building at 2112 Quimby Ave, Bronx, New York.

VI. Suriel and 309 Wyckoff

61. On or about the morning of December 16, 2024, law enforcement learned that UPS had intercepted, held, and opened three packages sent from Florida to 309 Wyckoff. The packages contained electronic devices. Law enforcement took possession of one of these packages which contained Apple products, including four iPhones and ten sets of Apple Air Pods. After confirming with the mobile phone provider that multiple of these devices were stolen in route to customers, law enforcement engaged in a controlled delivery of the stolen devices to 309 Wyckoff. At approximately 4:45 p.m., a law enforcement officer dressed as a UPS delivery driver delivered the UPS package containing stolen electronic devices to a Wyckoff Wireless employee ("Wyckoff Employee-1") at 309 Wyckoff.

62. A review of surveillance video from a pole camera at 309 Wyckoff shows that on or about December 16, 2024, at approximately 4:52 p.m., an unknown male ("UM1") wheeling a black carry-on bag was observed entering 309 Wyckoff. He handed the carry-on bag to Wyckoff Employee-1 who took it behind the counter. UM1 departed 309 Wyckoff at approximately 5:06 p.m. with the carry-on bag. At approximately 5:45 p.m., another unknown man ("UM2") entered 309 Wyckoff carrying a large white plastic bag and handing it to Wyckoff Employee-1. At approximately 5:51 p.m., UM2 collected a small white envelope from Wyckoff Employee-1. At approximately 5:56 p.m., **Suriel** entered 309 Wyckoff. **Suriel,** the store owner, used a code to open the glass door leading to a back room at 309 Wyckoff and carried boxes into the back room with Wyckoff Employee-1.

63. At approximately 6:17 p.m., **Marte Tavares** entered 309 Wyckoff carrying a large blue paper bag and a large black plastic bag. **Marte Tavares** handed the two bags to Wyckoff Employee-1 who brought them behind the counter. At approximately 6:28 p.m., **Suriel** exited 309 Wyckoff carrying what appeared to be the same blue bag delivered by **Marte Tavares**. **Marte Tavares's** vehicle cannot be seen in this video at 309 Wyckoff. However, license plate reader ("LPR") data shows that at approximately 4:05 p.m., the **Marte Tavares** Vehicle was on the Throgs Neck Expressway Northbound Lane in the Bronx. At approximately 4:53 p.m., the **Marte Tavares** Vehicle was at the intersection of North Central Avenue and Hendricks Avenue in Valley Stream, New York. At 7:02 p.m., the **Marte Tavares** Vehicle was

heading Bronx-bound on the Robert F. Kennedy Bridge. As set forth in Section V above, the **Marte Tavares** vehicle was observed parked in front of 2227 University in the Bronx at 7:45 p.m.

64. As part of the investigation that led to **Suriel's** guilty plea in the District of Kansas in United States v. Joel Suriel, a/k/a "La Melma", 18-CR-20028, a witness identified **Suriel** as the owner of Wyckoff Wireless engaged in the sale of stolen phones. The witness also identified **Suriel's** nickname as "La Melma." The witness also provided a phone number ending in -5812 (the '**Suriel Phone**") as **Suriel's**.

65. As set forth in Section VII below, evidence analyzed from seized phones, including from **Montero Hernandez**, shows that **Suriel** ("La Melma") operates 309 Wyckoff as a location for the large-scale purchase of stolen electronic devices.

VII. Montero Hernandez, Diaz Dominguez, and Nunez Ship Stolen Devices to Suriel at 309 Wyckoff

66. On or about October 10, 2024, FedEx contacted HSI regarding a suspicious package. A customer identifying himself as "**Luis Nunez**" walked into a FedEx store in Illinois to ship a package of what he declared as "baby clothes" to a FedEx site in Moonachie, New Jersey. A FedEx employee notified security to inspect. FedEx security opened the box and found it filled with brand new iPhones, which were later determined to be stolen. Subsequent review of the security video from the Illinois FedEx store showed both **Nunez** and **Diaz Dominguez** at the location arranging the shipment.

67. On or about October 11, 2024, the listed shipper identifying himself as **Luis Nunez** called FedEx to complain that the recipient received the shipment, but that it was empty and only filled with paper. The caller called from a number ending in -9833 (the "**Diaz Dominguez** Phone"). The **Diaz Dominguez** Phone is registered to **Diaz Dominguez**. Further, investigation revealed that **Diaz Dominguez** provided the same phone number to NYPD when he was the victim of a robbery. The caller stated that he is in the business of buying and selling iPhones and that the package contained 30-40 iPhones. The caller called FedEx again later that day and complained that someone stole his iPhones.

68. According to FedEx records and security video footage, on or about November 1, 2024, **Nunez** and **Diaz Dominguez** entered a FedEx store in Colorado and paid $779.38 to ship a package to 309 Wyckoff. The shipper was again listed as "**Luis Nunez**". FedEx security inspected the package and found: 22 iPhones, a Samsung Galaxy phone, four Apple Watches, four iPads, and four MacBook Pro computers. Each of these devices was subsequently confirmed as stolen.

69. On or about September 9, 2024, **Montero Hernandez** was arrested in Cranford, New Jersey for a package theft. During his arrest, a phone (the "**Montero**

Hernandez Phone") was seized and subsequently searched pursuant to a warrant. A review of the **Montero Hernandez** Phone showed that **Montero Hernandez** travels around the country with **Nunez** and **Diaz Dominguez,** stealing packages of electronic devices and shipping them in bulk, frequently to Wyckoff Wireless. Further, the review showed that **Montero Hernandez, Nunez,** and **Diaz Dominguez** are also involved in obtaining electronic devices through fraudulent orders.

70. Review of the **Montero Hernandez** phone further showed that **Montero Hernandez** used an encrypted messaging application to chat with **Diaz Dominguez**, using the number assigned to the **Diaz Dominguez** Phone. They discussed using a "dialer," which is commonly employed in call center schemes to obtain personally identifiable information. Using this information, new phones can be added to accounts and the shipments tracked for shipment. **Montero Hernandez** and an individual in the Dominican Republic ("Co-Conspirator-3") also communicated about various short-term vacation rentals across the country.

71. On or about July 5, 2023, **Montero Hernandez** texted **Diaz Dominguez** asking how much "melma" (**Suriel**), would pay for an "unlock", referring to activation of a stolen phone. On or about July 10, 2024, **Montero Hernandez** sent **Diaz Dominguez** a list of devices and specifications including approximately 14 iPhones and multiple other electronic devices. **Montero Hernandez** told **Diaz Dominguez** to send the list to "La Melma" (**Suriel**). **Diaz Dominguez** responded with the prices for the devices.

72. **Montero Hernandez** and **Diaz Dominguez** also communicated regarding shipments of stolen devices to 309 Wyckoff. On or about June 17, 2024, **Montero Hernandez** sent **Diaz Dominguez** a FedEx receipt showing a shipment from Oklahoma to 309 Wyckoff, followed by a list of the items shipped including 12 iPhones, 2 Samsung phones, and 2 Apple Watches. Law enforcement discovered additional messages regarding shipments to Wyckoff Wireless and FedEx receipts showing these shipments were sent on or about September 18, 2023, October 3, 2023, November 8, 2023, and August 2, 2024.

73. Review of the **Montero Hernandez** Phone also revealed text conversations between **Montero Hernandez** and **Nunez**, using a phone number ending in -2222 (the "**Nunez** Phone"). Between on or about June 24, 2023, and on or about September 18, 2024, there were approximately 7,960 messages between the two, including photos of **Nunez** and **Montero Hernandez** socializing together, an image of a bank card in **Nunez**'s name, and a New York Department of Motor Vehicles customer receipt for **Nunez**. The review also showed multiple FedEx receipts of large (approximately 20 pounds or more) packages being sent to 309 Wyckoff and photos of electronic devices. The FedEx shipping receipts show that shipments of stolen devices were being sent via FedEx from around the country, including California, Arizona, Nevada, and Utah.

74. Review of the **Montero Hernandez** Phone also showed that Co-Conspirator-3 supplied **Montero Hernandez** and **Diaz Dominguez** with tracking numbers and addresses. The review showed that **Montero Hernandez** pays a percent of the sale of the devices to Co-Conspirator-3.

VIII. Vazquez Sanchez and the BotTrack Telegram Channel

75. A Telegram "channel" is a way to send messages to a large group of people on the Telegram encrypted messaging application. One Telegram channel named "BotTrack" offers tracking and delivery information for sale. Law enforcement has monitored "BotTrack" and purchased this information.

76. On or about October 22, 2024, while in New Jersey, UC1 negotiated in Spanish with the Telegram user who runs the BotTrack Telegram channel. They agreed on a price of $50 in Bitcoin for delivery addresses and customer names for two FedEx tracking numbers in the area of Newark, New Jersey. UC1 sent the Bitcoin payment to a Bitcoin address provided by the Telegram user (the "BotTrack Bitcoin Address"). The Telegram user then sent UC1 a file named "NJ.txt", which was a text file containing the two tracking numbers and including city and state of origin, city and state of destination, weight, and dimensions. On or about October 23, 2024, UC1 selected two tracking numbers from a new list provided, and the Telegram user responded with full customer names and addresses for customers in Newark and Milford, New Jersey.

77. On or about November 12, 2024, a confidential informant ("CI1"), while in the presence of law enforcement, attempted to purchase five tracking numbers from the Telegram user who runs the BotTrack channel. Law enforcement paid $150 in Bitcoin to the BotTrack Bitcoin Address but CI1 did not receive the addresses. After continued communication, on November 13, 2024, CI1 selected five tracking numbers listed for Newark and received five addresses and customer names in Newark. Even though CI1 had already paid, the Telegram user requested additional payment via a peer-to-peer payment application. The peer-to-peer payment was requested to an account listed as an Apple iCloud account in **Lora Castillo's** name.

78. After obtaining the Newark delivery addresses, law enforcement contacted FedEx and arranged to take possession of a new iPhone. Law enforcement photographed the box, the phone and the Victim-1 packing slip. At approximately 2:30 p.m., the BotTrack Telegram user directed CW1 to take the stolen phone to a fence location in the Bronx (not 2227 University). At approximately 4:50 p.m, CW1 entered a store in the Bronx where CW1 exchanged the "stolen" iPhone for $400.

79. Review of a phone seized from a runner ("Runner-2") arrested during a package theft shows the runner sent money to **Vazquez Sanchez**'s wife's peer-to-peer payment account. Records from the peer-to-peer payment application show that

Vazquez Sanchez's wife's account converted money to Bitcoin and sent it to the BotTrack Bitcoin Address. The wife's account also sent money to a peer-to-peer payment account in **Vazquez Sanchez**'s name. **Vazquez Sanchez**'s peer-to-peer payment account also attempted a $1 test transaction to an account in **Lora Castillo**'s name, but it was rejected.

80. A different runner ("Runner-3") arrested for package theft identified **Vazquez Sanchez** as directing his criminal activities. According to Runner-3, he traveled to different locations to steal packages and **Vazquez Sanchez** paid for his travel expenses.

81. A lawful review of data on Runner-3's phone confirms this. Runner-3 communicated via an encrypted messaging application with **Vazquez Sanchez** via a phone number in **Vazquez Sanchez**'s true name. Further, the photo for this contact in Runner-3's phone is a photo of **Vazquez Sanchez**. Between March and June 2024, **Vazquez Sanchez** sent Runner-3 over 100 names, addresses, weights, and dimensions of packages for theft. The phone review also confirmed that **Vazquez Sanchez** was paying Runner-3's travel expenses. Over 20 of these tracking numbers have been confirmed stolen.

IX. Duverge Guzman

82. A review of evidence from a phone seized from Runner-1 shows that **Duverge Guzman** uses two different phone numbers for his communications with Runner-1 via an encrypted messaging application. First, **Duverge Guzman** uses a phone number ending in -9385 ("**Duverge Guzman** Phone-1"). During conversations between Runner-1 and **Duverge Guzman** Phone-1, Runner-1 calls the user of **Duverge Guzman** Phone-1 Fred or Frederick. The conversations also include photos and videos of Runner-1 and **Duverge Guzman** socializing. A second phone ending in -9951 ("**Duverge Guzman** Phone-2") also contain photos of Runner-1 and **Duverge** socializing and Runner-1 refers to him as Fred or Frederick. The contact names for both the phones are listed as "F" in Runner-1's phone. A lawful review of Runner-1's phone shows that **Duverge Guzman** sent Runner-1 over 100 tracking numbers of addresses for theft.

83. **Duverge Guzman** also has a third phone number ending in -2339 ("**Duverge Guzman** Phone-3"). On or about December 9, 2024, **Duverge Guzman** was a passenger in a car involved in an accident. When interviewed by NYPD, he provided **Duverge Guzman** Phone-3 as his phone number.

84. Law enforcement has monitored a lawfully authorized pen register and trap and trace device ("PRTT") on the encrypted-messaging account registered to the **Jerez** Phone. Between on or about December 27, 2024, and on or about February 13, 2025, there have been approximately 366 communications between the **Jerez** Phone and **Duverge Guzman** Phone-3.

X. Pen Register and Trap and Trace Data

85. According to queries of databases using public records, a number ending in -7634 (the "**Marte Tavares** Phone") is associated with **Marte Tavares** and a Social Security number associated with **Marte Tavares**. In addition, the **Marte Tavares** Phone and the **Marte Tavares** Vehicle are both registered using the same home address, and the **Marte Tavares** Vehicle is registered in **Marte Tavares**'s true name.

86. Analysis of PRTT data shows that between on or about November 18, 2024, and on or about February 10, 2025, the **Jerez** Phone and the **Marte Tavares** Phone communicated 10,772 times.

87. According to communications reviewed pursuant to the warrant on **Montero Hernandez's** phone, **Montero Hernandez** and **Diaz Dominguez's** conversations referenced a phone number ending in -3157 ("**Suriel** Phone-2") being used by "La Melma" (**Suriel**) at 309 Wyckoff.

88. Analysis of the PRTT data shows that between on or about November 20, 2024 and on or about February 3, 2025, the **Jerez** Phone and **Suriel** Phone-2 communicated 632 times.

89. According to a review of CW1's phone, **Lora Castillo** has used two different phone numbers ending in -7079 ("**Lora Castillo** Phone-1") and -2965 ("**Lora Castillo** Phone-2").

90. Analysis of the PRTT data shows that on or about January 29, 2025, **Lora Castillo** Phone-2 and **Suriel** Phone-2 communicated 9 times. Between on or about October 24, 2024, and on or about November 8, 2024, **Lora Castillo** Phone-1 and **Suriel** Phone-2 communicated 19 times.

91. Analysis of the PRTT data shows that between on or about January 24, 2025, and on or about February 14, 2025, the **Jerez** Phone and **Lora Castillo** Phone-2 communicated 143 times. Further, between on or about October 23, 2024, and on or about November 8, 2024, the **Jerez** Phone and **Lora** Phone-1 communicated 44 times.