

---

---

UNITED STATES DISTRICT COURT  
DISTRICT OF NEW JERSEY

---

---

UNITED STATES OF AMERICA	:	Hon. James B. Clark, III
	:	
v.	:	Mag. No. 20-12414
	:	
AARON LLODY NORTHERN,	:	
a/k/a "Bossdon Butta,"	:	
COREY BOND,	:	
a/k/a "Teddy Brown,"	:	
TYRELL BAKER,	:	
ANDRE TYRONE WALLACE,	:	
MICHELLIAN THOMPSON,	:	
ACHIEL MORGAN,	:	
a/k/a "Ace Skrap,"	:	
QUINTON SESSIONS,	:	
a/k/a "Q Doggy Widda Hoddie,"	:	
BRIAN ADJAVON,	:	
a/k/a "CarlosSlimm,"	:	<b><u>CRIMINAL COMPLAINT</u></b>
a/k/a "sasuforever,"	:	
DASHAWN DANFORTH,	:	
a/k/a "Shawn Moneyy Marley,"	:	
SIMONE CORDERO,	:	
STEPHANIE LEE SANCHEZ,	:	
HANS PIERRE,	:	
a/k/a "hustlehans"	:	

I, Ryan Gale, 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 Postal Inspector with the United States Postal Inspection Service, and that this complaint is based on the following facts:

**SEE ATTACHMENT B**

Continued on the attached pages and made a part hereof:

---

Inspector Ryan Gale  
U.S. Postal Inspector Service

Attested to me by telephone pursuant to Federal Rule of Criminal Procedure  
4.1(b)(2)(A) on October 21, 2020, in the District of New Jersey.

HONORABLE JAMES B. CLARK, III  
UNITED STATES MAGISTRATE JUDGE

---

Signature of Judicial Officer

**ATTACHMENT A**

**Count One**  
**Bank Fraud Conspiracy**

From in or about January 2018 through in or about December 2019, in Essex County, in the District of New Jersey and elsewhere, the defendants,

AARON LLODY NORTHERN,  
a/k/a "Bossdon Butta,"  
COREY BOND,  
a/k/a "Teddy Brown,"  
TYRELL BAKER,  
ANDRE TYRONE WALLACE,  
MICHELLIAN THOMPSON,  
ACHIEL MORGAN,  
a/k/a "Ace Skrap,"  
QUINTON SESSIONS,  
a/k/a "Q Doggy Widda Hoddie,"  
BRIAN ADJAVON,  
a/k/a "CarlosSlimm,"  
a/k/a "sasuforever,"  
DASHAWN DANFORTH,  
a/k/a "Shawn Moneyy Marley,"  
SIMONE CORDERO,  
STEPHANIE LEE SANCHEZ, and  
HANS PIERRE,  
a/k/a "hustlehans"

did knowingly and intentionally conspire and agree with each other and others to execute a scheme and artifice to defraud a financial institution, as defined in Title 18, United States Code, Section 20, namely, Bank-1, Bank-2, Bank-3, Bank-4, Bank-5, Bank-6, Bank-7, Bank-8, Bank-9, Bank-10, and Bank-11 whose deposits were insured by the Federal Deposit Insurance Corporation, and to obtain monies, funds, assets, and other property owned by and under the custody and control of Bank-1, Bank-2, Bank-3, Bank-4, Bank-5, Bank-6, Bank-7, Bank-8, Bank-9, Bank-10, and Bank-11 by means of materially false and fraudulent pretenses, representations, and promises, contrary to Title 18, United States Code, Section 1344.

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

**Count Two**  
**Conspiracy to Receive and Possess of Stolen Mail**

From in or about August 2018 through in or about December 2019, in Essex County, in the District of New Jersey and elsewhere, the defendants,

AARON LLODY NORTHERN,  
a/k/a "Bossdon Butta,"  
COREY BOND,  
a/k/a "Teddy Brown,"  
TYRELL BAKER,  
ANDRE TYRONE WALLACE,  
MICHELLIAN THOMPSON,  
ACHIEL MORGAN,  
a/k/a "Ace Skrap,"  
QUINTON SESSIONS,  
a/k/a "Q Doggy Widda Hoddie,"  
BRIAN ADJAVON,  
a/k/a "CarlosSlimm,"  
a/k/a "sasuforever,"  
DASHAWN DANFORTH,  
a/k/a "Shawn Moneyy Marley,"  
SIMONE CORDERO,  
STEPHANIE LEE SANCHEZ, and  
HANS PIERRE,  
a/k/a "hustlehans"

did knowingly and intentionally conspire and agree with each other and others to buy, receive, conceal, and unlawfully have in their possession, any letter, postal card, package, bag, and mail, and any article and thing contained therein, which has been so stolen, taken, embezzled, and abstracted, as herein described, knowing the same to have been stolen, taken, embezzled, and abstracted, contrary to Title 18, United States Code, Section 1708.

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

**Count Three**  
**Conspiracy to Possess and Receive Interstate Altered Securities**

From in or about August 2018 through in or about December 2019, in Essex County, in the District of New Jersey and elsewhere, the defendants,

AARON LLODY NORTHERN,  
a/k/a "Bossdon Butta,"  
COREY BOND,  
a/k/a "Teddy Brown,"  
TYRELL BAKER,  
ANDRE TYRONE WALLACE,  
MICHELLIAN THOMPSON,  
ACHIEL MORGAN,  
a/k/a "Ace Skrap,"  
QUINTON SESSIONS,  
a/k/a "Q Doggy Widda Hoddie,"  
BRIAN ADJAVON,  
a/k/a "CarlosSlimm,"  
a/k/a "sasuforever,"  
DASHAWN DANFORTH,  
a/k/a "Shawn Moneyy Marley,"  
SIMONE CORDERO,  
STEPHANIE LEE SANCHEZ, and  
HANS PIERRE,  
a/k/a "hustlehans"

did knowingly and intentionally conspire and agree with each other and others to receive, posses, conceal, store, barter, sell, and dispose of any falsely made, forged, altered, and counterfeited securities, moving as, and which are a part of, and which constitute interstate and foreign commerce, knowing the same to have been so falsely made, forged, altered, and counterfeited, contrary to Title 18, United States Code, Section 2315.

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

**Count Four**  
**Money Laundering Conspiracy**

From in or about August 2018 through in or about February 2019, in Essex County, in the District of New Jersey and elsewhere, the defendants,

AARON LLODY NORTHERN,  
a/k/a "Bossdon Butta,"  
QUINTON SESSIONS,  
a/k/a "Q Doggy Widda Hoddie,"  
BRIAN ADJAVON,  
a/k/a "CarlosSlimm,"  
a/k/a "sasuforever,"  
DASHAWN DANFORTH,  
a/k/a "Shawn Moneyy Marley," and  
HANS PIERRE,  
a/k/a "hustlehans"

did knowingly and intentionally conspire and agree with each other and others to conduct and attempt to conduct a financial transaction affecting interstate and foreign commerce, which involved the proceeds of specified unlawful activity while knowing that the property involved in the financial transaction represented the proceeds of some form of unlawful activity and knowing that the transactions were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of said specified unlawful activity, contrary to Title 18, United States Code, Section 1956(a)(1)(B)(i).

In violation of Title 18, United States Code, Section 1956(h).

**Count Five**  
**Aggravated Identity Theft**

On or about February 22, 2019, in Union County, in the District of New Jersey, and elsewhere, the defendants,

SIMONE CORDERO, and  
HANS PIERRE,  
a/k/a “hustlehans”

did knowingly possess and use, without lawful authority, a means of identification of another person during and in relation to a felony violation enumerated in 18 U.S.C. § 1028A(c), to wit, bank fraud conspiracy contrary to Title 18, United States Code, Section 1349, knowing that the means of identification belonged to another actual person.

In violation of Title 18, United States Code, Section 1028A(a)(1).

## **ATTACHMENT B**

I, Ryan Gale, am a Postal Inspector with the U.S. Postal Inspection Service ("USPIS"). I have knowledge about the facts set forth below from my involvement in the investigation, my review of reports, documents, pictures, videos, witness interviews, and discussions with other law enforcement officials. Because this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact that I know concerning this investigation. All statements described herein are relayed in substance and in part. When dates and times are alleged herein, those dates and times are approximate.

1. USPIS has been investigating a group of individuals who stole checks taken from the mail, altered the payee and/or amount on stolen checks, possessed and transported the stolen and altered checks outside of New Jersey through interstate commerce, fraudulently took money from banks that did not belong to them, and then laundered the stolen money by concealing it through different financial accounts.

2. Through the course of the investigation, USPIS has received complaints from several individuals and entities who placed checks in the mail at United States Postal Service ("USPS") collection boxes in the Newark, New Jersey area and beyond. These complainants placed checks in the mail, and those checks were subsequently altered and deposited into accounts that did not belong to the intended recipient and for amounts that were not originally written on the checks. USPIS has also received complaints from individuals who placed their checks in their personal mailboxes outside of their homes, who then had their checks stolen and deposited into other individuals' and entities' bank accounts.

3. Law enforcement has collected and reviewed surveillance footage from certain dates during the course of the conspiracy that depict certain USPS collection boxes located in Newark, New Jersey. That surveillance footage shows one or more individuals stealing mail from the USPS collection boxes at night.

4. At all times relevant to this Complaint, Bank-1, Bank-2, Bank-3, Bank-4, Bank-5, Bank-6, Bank-7, Bank-8, Bank-9, Bank-10, and Bank-11 were federally insured "financial institutions," as that term is defined in 18 U.S.C. § 20.

5. Throughout the course of the scheme described herein, certain defendants transferred illegally obtained funds to one another through "Cash App," a web application provided by Square, Inc. Cash App is an application that one downloads onto an iOS or Android device. Once downloaded, the user then provides the application his or her mobile number or email to create a unique username, which the company refers to as a "\$Cashtag." Creation of a \$Cashtag automatically creates a shareable web address through which others can make payments. The application also allows users to link a bank account or debit card information to the account.

6. Throughout the course of the scheme described herein, some of the

defendants also transferred illegally obtain funds to one another through Zelle, an electronic money transfer program. A Zelle user can transfer money by enrolling an email account or mobile number, either through certain mobile banking applications or through Zelle's application. After registering, to transfer money, the user enters the preferred email address or mobile number of the recipient and the amount the user wants to transfer to that recipient.

7. During the course of the scheme described herein, law enforcement has identified at least two phone numbers that were in contact with several members of the conspiracy. According to phone records, an account corresponding to a phone number ending in 5711 (hereinafter, the "5711 Phone Number") was activated on or about January 22, 2018 and closed on or about April 17, 2019. The name of the subscriber of this account was "Carlos Slim." An account corresponding to a phone number ending in 0998 (hereinafter, the "0998 Phone Number") was activated on or about October 10, 2018, in the subscriber name of "Barlos Blim."

### **Evidence of Connections Among the Defendants**

8. Several of the defendants utilize, and are connected with one another on, social media. As a part of the investigation, law enforcement obtained information regarding certain Facebook and Instagram accounts.

9. It appears that certain defendants maintain social media accounts and have interacted with one another using those accounts, as follows:

- a. Law enforcement believes that a Facebook account with the display name "Bossdon Butta" (the "Bossdon Butta Account") is controlled by defendant AARON LLODY NORTHERN ("NORTHERN"). The public-facing photographs used as the profile pictures for the Bossdon Butta Account depict NORTHERN.
- b. Law enforcement believes that a Facebook account bearing username "CarlosSlimm" and display name "Mpere Bri" (the "Carlos Slimm Account") is controlled by defendant BRIAN ADJAVON ("ADJAVON"). The Carlos Slimm Account contains a profile picture and several other photos of a man who appears to be ADJAVON. In communications with some of the coconspirators, it appears that ADJAVON's friends refer to him as "bri," likely short for "Brian," ADJAVON's first name. Further, the user of the Carlos Slimm Account posted "29 this year ain't no holding back" at a time when ADJAVON would have turned 29 that particular year. Additionally, the Bossdon Butta Account posted on the Facebook wall of the Carlos Slimm Account on or about a date known to be ADJAVON's birthday, sending the messages "Happy bday bro" and "Happy belated bday bro."
- c. Law enforcement believes that a Facebook account bearing display name "Teddy Brown" (the "Teddy Brown Account") is

controlled by defendant COREY BOND (“BOND”). The Teddy Brown Account contains photos that appear to be of BOND. The account also posted a screenshot on or about January 23, 2019, which appears to be an email that says, in relevant part, “Cory, thanks for reaching out to us.”

- d. Law enforcement believes that a Facebook account bearing the display name “Andre Tyrone Wallace” (the “Wallace Account”) is controlled by defendant ANDRE TYRONE WALLACE (“WALLACE”). The public-facing photographs on the Wallace Account appear to be of WALLACE.
- e. Law enforcement believes that a Facebook account bearing the display name “Ace Skrap” (the “Ace Skrap Account”) is controlled by defendant ACHIEL MORGAN (“MORGAN”). The background photo on this account depicts a male individual that appears to be MORGAN. Additionally, other Facebook accounts that appear to have also been controlled by MORGAN also use the alias “Ace Skrap.”
- f. Law enforcement believes that a Facebook account bearing a display name “Quinton Sessions (Q Doggy Widda Hoodie),” (the “Q Doggy Account”) is controlled by defendant QUINTON SESSIONS (“SESSIONS”). The photos posted on the Q Doggy Account appear to be of SESSIONS.
- g. Law enforcement believes that a Facebook account with the display name “Shawn Moneyy Marley” (the “Moneyy Marley Account”) is controlled by defendant DAYSHAWN DANFORTH (“DANFORTH”). The Moneyy Marley Account has photos posted that appear to be DANFORTH.
- h. Law enforcement believes than an Instagram account with the display name “hustlehans” (the “hustlehans Account”) is controlled by defendant HANS PIERRE (“PIERRE”). The verified phone number listed on the hustlehans Account is the same phone number listed on PIERRE’s Cash App account. The hustlehans Account has several photographs that depict PIERRE. In addition, “Hustle Hans” is the name that PIERRE uses as his rap moniker and is displayed in text at the bottom of the beginning of a video for PIERRE’s rap performance titled “Cash App,” which was posted on the Internet.
- i. Law enforcement believes that the Instagram account that once used the display name “sasuforever” (the “sasuforever Account”) is controlled by defendant ADJAVON. The sasuforever Account depicts photographs of a man who appears to be ADJAVON. On or about August 15, 2019, the sasuforever Account commented on

a photo of PIERRE uploaded to the hustlehans Account, “Hustle hannnnssssssssss,” to which user hustlehans replied, “@sasuforever My guy bri.” Again, law enforcement believes that “bri” is likely a reference to “Brian,” ADJAVON’s first name.

- j. The Carlos Slimm Account is Facebook “friends” with the Q Doggy Account, the Bossdon Butta Account, the Moneyy Marley Account, and the Wallace Account. Further the Carlos Slimm Account and the Ace Skrap Account communicated with one another on Facebook.
- k. The Wallace Account and the Moneyy Marley Account are Facebook “friends” with one another. Further, the Wallace Account and the Moneyy Marley Account communicated with one another via Facebook messenger regarding the scheme described herein.
- l. The Q Doggy Account is Facebook “friends” with the Teddy Brown Account and the Bossdon Butta Account.
- m. In or around 2016, a Facebook user posted a photograph depicting ADJAVON and PIERRE standing next to one another.

10. According to records from the New York Department of Motor Vehicles (“NY DMV”), SESSIONS resides in the same neighborhood in the Bronx, New York (the “Neighborhood”), as WALLACE and defendant TYRELL BAKER (“BAKER”). Banking records also indicate that ADJAVON’s listed address is in the Neighborhood. Additionally, MORGAN and another person referenced herein (the “Roommate”) shared the same listed address in or around 2019.

### **AARON LLODY NORTHERN**

11. Based on the investigation, NORTHERN has utilized several bank accounts in furtherance of the scheme and allowed one or more coconspirators to deposit stolen, altered checks into his accounts.

12. NORTHERN maintained the following bank accounts that were used in furtherance of the fraud described herein.

- a. NORTHERN utilized a bank account at Bank-3 in furtherance of the fraud (the “Northern Bank-3 Account”), which he opened in approximately 2012. NORTHERN was the only authorized signatory on the account.
- b. On or about May 11, 2018, NORTHERN opened a bank account with Bank-2 (the “Northern Bank-2 Account”). NORTHERN was the only authorized signatory on the account.
- c. On or about September 22, 2018, NORTHERN opened a bank account with Bank-4 (the “Northern Bank-4 Account”). NORTHERN was the only authorized signatory on the account.

### **Check from Individual Victim-1**

13. On or about September 12, 2018, a check drawn on an account at Bank-1 belonging to an individual ("Individual Victim-1") was deposited into the Northern Bank-2 Account in Mamaroneck, New York. When deposited, the check displayed that it was to be paid to the order of "Aaron L. Northern" in the amount of \$9,800 and reflected in the memo line that the check was for a "car deposit."

14. According to Individual Victim-1, Individual Victim-1 placed the aforementioned check in the mail in Newark, New Jersey. When Individual Victim-1 placed the check in the mail, the check was made payable to an Internet service provider and was payable in the amount of approximately \$140.

### **Check from Individual Victim-2**

15. On or about September 18, 2018, a check bearing a New Jersey address drawn on an account at Bank-1 belonging to an individual ("Individual Victim-2") was deposited into the Northern Bank-3 Account at an ATM machine in New York, New York. When deposited, the check displayed that it was to be paid to the order of "Aaron L. Northern" in the amount of \$9,750.

16. According to Individual Victim-2, Individual Victim-2 placed the aforementioned check in the mail in a collection box in Newark, New Jersey. When Individual Victim-2 placed the check in the mail, the check was made payable to an insurance company and was payable in the amount of approximately \$189.

### **Check from Victim Company-1**

17. On or about September 24, 2018, a check drawn on a business account at Bank-1 belonging to a company ("Victim Company-1") was deposited into the Northern Bank-2 Account in Mamaroneck, New York. When deposited, the check displayed that it was to be paid to the order of "Aaron L. Northern" in the amount of \$15,050.

18. According to a representative of Victim Company-1, the check described in the aforementioned paragraph was not originally made payable to "Aaron Northern." Victim Company-1 placed the check in the mail in or around Newark, New Jersey to be sent and payable to someone other than Aaron Northern.

### **Check from Individual Victim-3**

19. On or about September 24, 2018, a check drawn on an account at Bank-1 belonging to an individual ("Individual Victim-3") was deposited into the Northern Bank-3 Account at an ATM in New York, New York. When deposited, the check displayed that it was to be paid to the order of "Aaron L. Northern" in the amount of \$9,800.

20. According to Individual Victim-3, Individual Victim-3 placed the aforementioned check in the mail in a collection box in Newark, New Jersey.

When Individual Victim-3 placed the check in the mail, the check was payable to a phone company and was payable in the amount of approximately \$63.

**Check from Individual Victim-4**

21. On or about September 27, 2018, a check bearing a New Jersey address drawn on an account at Bank-1 belonging to an individual (‘Individual Victim-4’) was deposited into the Northern Bank-3 Account in New York, New York. When deposited, the check displayed that it was to be paid to the order of ‘Aaron L. Northern’ in the amount of \$9,800.

22. According to Individual Victim-4, Individual Victim-4 placed the aforementioned check in the mail in a collection box in Newark, New Jersey. When Individual Victim-4 placed the check in the mail, the check was payable to the United States Department of the Treasury (‘U.S. Treasury’) and was payable in the amount of approximately \$2,750.

**Other NORTHERN Transactions and Communications**

23. According to the records from the Northern Bank-3 Account:

- a. On or about September 19, 2020, funds in the approximate amount of \$1,003 were withdrawn from the Northern Bank-3 Account at an ATM in the Bronx, New York.
- b. On or about September 19, 2020, two purchases were made from a post office in the Bronx, New York, in the amounts of \$1001.65 and \$991.65. For the reasons discussed below, it appears that these purchases were for money orders.

24. According to records from the Northern Bank-4 Account:

- a. On or about September 22, 2018, NORTHERN opened the Northern Bank-4 Account as the sole signatory.
- b. On or about September 24, 2018, two money orders—one in the amount of \$1,000 and the other in the amount of \$990—were deposited into the Northern Bank-4 Account. The money orders were both dated September 19, 2018 and were issued by the USPS. Both money orders were payable to Aaron Northern and bore a return address in the Neighborhood.
- c. On or about October 2, 2018, two money orders—one in the amount of \$1,000 and the other in the amount of \$990—were again deposited into the Northern Bank-4 Account. The money orders were both dated September 25, 2018 and were issued by the USPS. Both money orders were payable to Aaron Northern and bore an address in the Neighborhood.

25. On or about September 25, 2018, NORTHERN’s Cash App account made three transfers to DANFORTH totaling approximately \$3,500. On or about October 4, 2018, NORTHERN’s Cash App account made two more transfers to

DANFORTH totaling approximately \$4,500. NORTHERN attempted to transfer more money to DANFORTH that day, but these transfers were either declined or blocked.

26. In or around October 4, 2018, surveillance footage from an ATM in Maryland reflected that NORTHERN made a cash withdrawal from the Northern Bank-3 Account. Two other cash withdrawals were made from the Northern Bank-3 Account that same day, also at locations in Maryland.

27. On or about October 30, 2018, the Q Doggy Facebook Account exchanged messages with the Bossdon Butta Account, with the Bossdon Butta Account asking user Q Doggy whether his Bank-2 account was “still good.”

28. On or about October 31, 2018, the Bossdon Butta Account messaged the Carlos Slimm Account twice directing ADJAVON to call NORTHERN.

### **COREY BOND**

29. The investigation has revealed that BOND conspired with others and allowed coconspirators to deposit fraudulent checks into his bank accounts.

### **Communications between BOND and SESSIONS**

30. On or about September 13, 2018, the Teddy Brown Account, believed to be utilized by BOND, and the Q Doggy Account, believed to be utilized by SESSIONS, exchanged the following messages:

Teddy Brown:	My shit is at a negative balance right now lemme get it above float
Teddy Brown:	Plus I'm in lower Eastside and I work 2 Jobs so I gotta find time too
Q Doggy:	THAT NEGATIVE DON'T MEAN NOTHING BRO
Q Doggy:	I WAS AT A NEGATIVE WEN I DANCED ON MY SHIT THE 2ND TIME
Teddy Brown:	You did it under Ya name ?
Q Doggy:	YEAA TWICE
Q Doggy:	GON DO IT AGAIN NEXT MONTH
Teddy Brown:	Aigh but I'm in LES doe I'm not in the Bronx no more and ain't U fuckin Ya Card callin [Bank-2 abbreviation] every month ? That's fake hot bro
Q Doggy:	IM DOING IT WIF PPLS UPSTATE , MARYLAND & DELAWARE
Q Doggy:	U GOOD
Q Doggy:	& NAHH BRO THAT'S THE THING NEGGAS GET SHAKEY OVER DISS SHIT WEN IT'S NOTHING TO GET

#### SHAKEY BOUT

Teddy Brown: Aigh ima fuck w. It how much I get & don't tell me a stack & niggas drop like 8 racks on my account

Q Doggy: IF NEGGAS DROP 8 U GETTING LIKE 5 & CHANGE MAYBE 6

Teddy Brown: Aigh U my Manz I trust you so ima fuck w. It Monday ?

Teddy Brown: I work at 1 so we'll do it in the morning

Q Doggy: SAYYDATT

Q Doggy: COPYY

31. On or about September 26, 2018, the two accounts continued the conversation on Facebook, with user Teddy Brown asking, "Is it same day cash out?," to which user Q Doggy replied, "GOTTA WAIT FEW DAYS FO CHECK TO CLEAR." Q Doggy asked Teddy Brown if he had a bank account or if he was opening one, to which Teddy Brown explained that he had a bank account by responding back with the abbreviation for Bank-2. Q Doggy responded, "OHH NEGGA U LITT" and "I JUST GOTTA PICK THAT UP FROM U."

32. Based on the investigation, law enforcement believes that the above is referencing the logistics of the scheme described herein.

#### **BOND Transactions**

33. On or about October 10, 2018, a check drawn on Bank-1 that reflected a New Jersey address on its face and that appeared to be payable for \$15,000 was deposited into a Bank-2 account controlled by BOND (the "Bond Bank-2 Account"). According to the entity that originally wrote the check ("Victim Company-2"), the check was originally made payable to someone other than BOND.

34. On or about January 14, 2019, a check drawn on Bank-6 that appeared to be payable to BOND in the amount of \$19,000 was deposited into a Bank-8 account controlled by BOND (the "Bond Bank-8 Account"). According to the Bank-6 accountholder ("Individual Victim-5"), the check was placed in a mailbox outside of his/her home, and the check, when placed in the mail, was written to be payable for Individual Victim-5's state income taxes, not to BOND.

35. According to bank and surveillance records, on or about January 30, 2019, BOND made a counter withdrawal from the Bond Bank-8 Account.

#### **TYRELL BAKER**

36. The investigation has revealed that BAKER has allowed coconspirator(s) to deposit stolen checks from the mail into his account.

37. On or about August 8, 2018, a check drawn on Bank-1 bearing a New Jersey address on its face that appeared to be payable to BAKER in the amount of

approximately \$6,400 was deposited into a Bank-7 bank account controlled by BAKER (the “Baker Bank-7 Account”). According to the entity that originally prepared the check (“Victim Company-3”), this check was placed in the mail in a collection box in Newark, New Jersey and was not mailed, or originally made payable, to BAKER. Prior to this deposit, Victim Company-3 placed three checks (including the check deposited into the Baker Bank-7 Account) in a collection box in Newark, New Jersey, but none of the three checks arrived at their intended destinations. The other two of the checks were deposited into accounts in the name of another person involved in the scheme (“Mule 1”).

38. As discussed further below, it appears that ADJAVON deposited the \$6,400 check described above into the Baker Bank-7 Account.

39. On or about September 4, 2018, approximately six checks were deposited into the Baker Bank-7 Account in the Bronx, New York. Each check appeared to be drawn on a Bank-7 account belonging to a doctor’s office in New York. Each check was payable to BAKER in the approximate amount of \$860.33. All six checks were returned as unpaid.

#### **ANDRE TYRONE WALLACE**

40. The investigation has revealed that Wallace allowed one of his bank accounts to be used in furtherance of the scheme described herein and posted evidence of the scheme described herein on social media.

41. On or about October 15, 2018, USPIS received a complaint from Individual Victim-2 referenced above. Individual Victim-2 stated that he/she had mailed three checks via a collection box in Newark, New Jersey. Individual Victim-2 reported that all three checks were altered and fraudulently deposited into accounts that did not belong to the intended recipients.

42. One of the three stolen checks, which was bore a New Jersey address on its face, was altered to reflect payment in the amount of \$9,800 payable to “Andre Wallace.” This check was deposited via ATM into a Bank-5 account belonging to WALLACE (the “Wallace Bank-5 Account”). Specifically, the check was deposited on or about September 10, 2018 at a Bank-5 location in Larchmont, New York. Prior to this deposit, the Wallace Bank-5 Account had no money in it.

43. On September 17, 2018, approximately \$2,000 was withdrawn from the Wallace Bank-5 Account from a Bank-5 ATM located in the Neighborhood. That same day, on September 17, 2018, surveillance footage reflects that WALLACE withdrew approximately \$6,700 in cash from this account from a Bank-5 bank located in the Bronx, New York. On September 18, 2018, \$620 in cash was withdrawn from a different Bank-5 ATM also located in the Neighborhood.

44. On December 12, 2018, the Wallace Account uploaded and posted onto Facebook a photograph of a man with his back to the camera in a red hooded sweatshirt standing in front of a Bank-5 ATM machine (the “Bank-5 Photo”). The

photo appears to have been taken at night. Law enforcement has compared Google Map photographs of the aforementioned Bank-5 locations in the Bronx, New York, as well as the aforementioned Bank-5 location in Larchmont, New York, and it appears that this photograph depicts an ATM consistent with the Bank-5 ATM located in Larchmont, New York, where the stolen and altered check described above was deposited into the Wallace Bank-5 Account. In other words, it appears that WALLACE posted onto his Facebook account a photograph of someone engaging in illegal activity via his Wallace Bank-5 Account.

### **MICHELLIAN THOMPSON**

45. The investigation has revealed that MICHELLIAN THOMPSON (“THOMPSON”) allowed her bank accounts to be used to deposit fraudulent checks and transferred money to at least one coconspirator in furtherance of the scheme. During the relevant time period, THOMPSON maintained a Bank-8 account (the “Thompson Bank-8 Account”) and a Bank-2 account (the “Thompson Bank-2 Account”), both of which were used to deposit checks that had been altered and stolen in connection with the scheme.

46. The Thompson Bank-2 account appears to have been maintained by THOMPSON prior to her involvement in this scheme and was opened in or around March 2017. The Thompson Bank-8 Account was opened in or around September 2018, with fraudulent check activity occurring in or around October and November 2018.

47. On or about August 8, 2018, a check bearing a New Jersey address on its face, drawn on Bank-1 in the approximate amount of \$14,050, which appeared to be payable to “Michellian C. Thompson,” was deposited into the Thompson Bank-2 Account at an ATM machine in Mamaroneck, New York. According to the person who originally wrote the check (“Individual Victim-6,”) Individual Victim-6 placed the check in the mail, which was not intended to be mailed, or payable to, THOMPSON.

48. On or about October 23, 2018, a check bearing a New Jersey address on its face, drawn on Bank-1, in the approximate amount of \$14,050, which appeared to be payable to “Michellian C. Thompson,” was deposited into the Thompson Bank-8 Account at an ATM in Larchmont, New York. The check was reported as stolen to the USPIS. According to the person who originally wrote the check (“Individual Victim-7”), the check was originally made payable to a local utility company in the amount of approximately \$34.49.

49. As discussed further below, surveillance footage from Bank-8 reflects that ADJAVON deposited this check into the Thompson Bank-8 Account.

50. On or about November 7, 2018, a check bearing a New Jersey address drawn on Bank-1, in the approximate amount of \$16,500 was altered to be payable to “Michellian Thompson,” was deposited into the Thompson Bank-8 Account, in Larchmont, New York via ATM. According to the individual who originally wrote the check (“Individual Victim-8”), the check was placed in a USPS

collection box in New Jersey and, at the time, was not written to be payable to THOMPSON.

51. According to records from Square, THOMPSON maintained a Cash App account which was used to transfer approximately \$1,900 to PIERRE on November 1, 2018 and which was used to attempt to transfer money to MORGAN.

### **ACHIEL MORGAN**

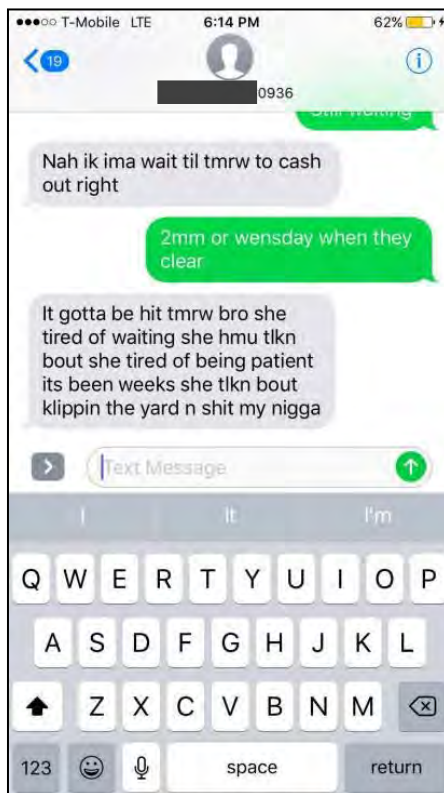
52. The investigation has revealed that MORGAN conspired with others in furtherance of the scheme herein and accepted financial payments derived from the fraudulently deposited and stolen checks.

53. As discussed above, MORGAN utilizes a Facebook account with the username "Ace Skrap." On or about January 1, 2018, the Ace Skrap Account, exchanged messages with the Carlos Slimm Account, which law enforcement believes is utilized by ADJAVON. The exchange is as follows:

Ace Skrap: Yo bri

CarlosSlimm: Ima call u

Ace Skrap:



CarlosSlimm: Ok

Ace Skrap: Wym [possibly, "what do you mean?"]

Ace Skrap: Hit me Asap

54. Based on the investigation, law enforcement believes that the

screenshot above, including the reference to “wait[ing]” until “when they clear,” is a reference to the fraud scheme described herein.

55. According to records from Square, as discussed above, THOMPSON’s Cash App account made several attempts to transfer money to MORGAN’s Cash App account during the approximate time period that fraudulent checks were being deposited into THOMPSON’s bank accounts.

56. On or about May 7, 2019, a check drawn on Bank-1 bearing a New Jersey address in the amount of \$15,050 (the “May 7 Check”) was deposited into a Bank-8 account (the “Mule 2 Account”) controlled by another person (“Mule 2”) at a location in Mamaroneck, New York. The May 7 Check was reported altered and stolen by the entity that originally wrote the May 7 Check (“Victim Company-4”). According to Victim Company-4, the May 7 Check was placed in the mail in Newark, New Jersey and was not intended to go to or be payable to Mule 2.

57. According to Mule 2, MORGAN, who Mule 2 knew by a different name but identified by photograph, contacted Mule 2 in or around April 2019. Following a conversation with MORGAN, Mule 2 was contacted by an unknown individual, who instructed Mule 2 to leave Mule 2’s debit card under a doormat on the side of a house in New York and was told that a check would be deposited into Mule 2’s account. Mule 2 provided the unknown individual the PIN number for Mule 2’s debit card. Thereafter, MORGAN called Mule 2 and told Mule 2 that the check had cleared. MORGAN, Mule 2, and an unknown individual went to Mule 2’s bank together. Mule 2 withdrew approximately \$8,000 from the account, which was derived from the May 7 Check and returned to MORGAN and the unknown individual. Mule 2 was permitted to keep \$1,000 and MORGAN and the unknown individual took the remainder of the cash.

### **QUINTON SESSIONS**

58. The investigation has revealed that SESSIONS recruited individuals to allow coconspirators to access and use bank accounts in furtherance of the scheme described herein.

59. As discussed above, BOND communicated with SESSIONS through Facebook in furtherance of the scheme described herein.

60. On or about August 24, 2018, a “Quinton Sessions” made a Visa Transfer of approximately \$2,500 into a bank account operated by another individual (“Mule 1”).

61. In or around September 2018, the Q Doggy Account exchanged messages with another individual on Facebook (“Mule 3”) about the scheme described herein:

Q Doggy: U GOT ANY BANK CARDS?

Mule 3: Yes but every time I do this, the person check always bounces and it turns out in result with opening a new

bank  
Q Doggy: U FW THE WRONG NEGGAS  
Mule 3: Right  
Mule 3: So what can i do.

In response, Q Doggy sent three screenshots, two of which appear to relate to an online Bank-2 account. One of the screens says "Hello, Michellian," and reflects a balance of approximately \$13,832.26.

Q Doggy: WHATCHU GOT  
Mule 3: So [Bank-2] is the one that be hitting ?  
Mule 3: I was thinking about opening a [Bank-2 abbreviation]  
Q Doggy: YEAA DEFF  
Mule 3: I had to close my [Bank-7 abbreviation] because like I said the dude check bounced  
Q Doggy: YA SHIT CUD BE NEW TOO  
Mule 3: So if I open it we do it?  
Q Doggy: YEAA I EVEN PAY YA OPEN U  
Q Doggy: \*UP

62. According to records received from Bank-2, on or about August 15, 2018, the beginning balance of the Thompson Bank-2 account was approximately \$13,832.26.

63. Further, on or about October 30, 2018, the Q Doggy Account exchanged messages with the Bossdon Butta Account, with the Bossdon Butta Account asking the Q Doggy Account whether his Bank-2 account was still good.

### **BRIAN ADJAVON**

64. The investigation has revealed that ADJAVON has deposited several of the fraudulent, stolen checks into others' bank accounts in connection with the scheme and appears to have communicated with his coconspirators in furtherance of the scheme.

65. A picture posted on or about August 30, 2018, on ADJAVON's Carlos Slimm Account reflects that ADJAVON has a large tattoo on his right forearm. On certain occasions, it appears that ADJAVON attempted to conceal his right arm to avoid detection by law enforcement.

66. Surveillance footage from Bank-7 shows an African-American male who law enforcement believes is ADJAVON hiding his right arm in a t-shirt and depositing a check into BAKER's Bank-7 account on August 8, 2018. As discussed above, this check was stolen and altered.

67. Surveillance footage from Bank-8 from on or about August 13, 2018 depicted an African-American male, who appeared to be ADJAVON, approach an ATM and hide his right arm behind his back. ADJAVON then deposited a stolen and altered check made payable to Mule 1 into a Bank-8 account (the “Mule Bank-8 Account”).

68. Surveillance footage from on or about August 30, 2018 from Bank-8 showed an African-American male who appears to be ADJAVON approach an ATM and deposit a stolen and altered check made payable to Mule 1 into the Mule Bank-8 Account. The surveillance footage depicted ADJAVON wearing a red and black jacket.

69. Surveillance footage obtained from Bank-2 reflected that the person who deposited the stolen and altered check referenced above from the Northern Bank-2 Account on or about September 12, 2018 also appears to be ADJAVON.

70. Surveillance footage from Bank-8 from on or about October 23, 2018 showed an African-American male who appeared to be ADJAVON wearing the same red and black jacket worn by ADJAVON on or about August 30, 2018, approach an ATM in Larchmont, New York. ADJAVON then deposited a stolen and altered check in the amount of \$14,050 into THOMPSON’s Bank-8 account.

71. As discussed above, ADJAVON and MORGAN communicated via Facebook about the timing of when someone should withdraw money that had cleared an account, which law enforcement believes was done in connection with this scheme.

72. Further, as discussed below, ADJAVON and PIERRE communicated via Instagram in furtherance of the scheme described herein.

73. On or about November 2, 2018, the Carlos Slimm Account messaged a Facebook account believed to be controlled by the Roommate who shared an address with MORGAN and told her: “Send ya number.”

74. On or about November 2, 2018, the 0998 Number called a phone number ending in 0101. That phone number is listed as the Roommate’s phone number on her Bank-9 bank account (the “Roommate Bank-9 Account”).

75. The address listed on the Roommate Bank-9 Account is the same address as the address listed by MORGAN on his driver’s license and one of his Cash App accounts.

76. On or about January 4, 2019, a check in the amount of approximately \$14,800.36 was deposited into the Roommate Bank-9 Account in Yonkers, New York. The check was drawn on Bank-1. The face of the check bore a New Jersey address and appeared payable to the Roommate. The check was returned as having been altered.

77. In addition, ADJAVON, using his Carlos Slimm Account, commented on the Wallace Account’s post of the Bank-5 Photo, described above, saying “This

pic is odeeeeeeee” and included a flame emoji. According to urbandictionary.com, the word “odee” is a Brooklyn-based slang term meaning “very.” The flame emoji is commonly used to reflect that something is “lit,” i.e., something is “exciting,” or “amazing.” Accordingly, it appears that ADJAVON commented that the Bank-5 Photo, which depicts the back of a man standing in front of an ATM at night, was “very” “amazing.” ADJAVON also “hearted” the post containing the Bank-5 Photo. To “heart” a particular post or comment on Facebook, in my training and experience, is to show approval for the post or comment.

78. According to records received from Square, ADJAVON sent and received transactions with the coconspirators via Cash App. For example, on or about February 22, 2019, ADJAVON received from “Hans Pierre” two transfers in the approximate amounts of \$1,870 and \$950. On or about February 23, 2019, ADJAVON received another transfer from “Hans Pierre” for approximately \$2,212.

### **DASHAWN DANFORTH**

79. It appears that throughout the course of the scheme, DANFORTH has received payments derived from the stolen, fraudulently deposited checks.

80. As discussed above, during August 2018, several fraudulently obtained and altered checks were deposited into the Northern Bank-3 Account, including checks deposited on or about September 18, 2018, and September 24, 2018.

81. On or about August 13, 2018, a stolen and altered check originally written by Victim Company-3, which appeared to be payable in the amount of \$9,350, was deposited into the Mule Bank-8 Account at an ATM in Larchmont Village, New York. This check was reported as having been stolen from a collection box in Newark, New Jersey.

82. On or about August 30, 2018, a stolen and altered check in the amount of \$6,800 was deposited into the Mule Bank-8 Account. This check was also reported as having been stolen from a collection box in Newark, New Jersey. From September 8, 2018 to October 7, 2018, another stolen and altered check in the amount of \$19,500 was deposited into Mule 1’s bank account.

83. Records also reflect that funds that Mule 1 transmitted electronically to DANFORTH were derived from the stolen altered checks that were fraudulently deposited into Mule 1’s bank account. On or about September 25, 2018, Mule 1 sent three successful Cash App payments to DANFORTH totaling approximately \$2,500.

84. On or about September 10, 2018, the Moneyy Marley Account, believed to be controlled by DANFORTH, communicated via Facebook with another person about the scheme (“Mule 4”). User Moneyy Marley instructed Mule 4: “Send yard,” “I’m wilding,” “Right now,” “Yeaaa bro kick an account,” and “I’m on fire.” Based on the investigation, law enforcement believes that DANFORTH was asking Mule 4 to provide DANFORTH with access to Mule 4’s bank account to

engage in the fraud scheme described herein.

85. On or about September 19, 2018 and September 25, 2018, the Northern Bank-3 Account transferred via Zelle approximately \$1,000 per transaction to a “Dashawn Dansforth.” Records from Bank-2 reflect that on or about September 19, 2018, September 25, 2018, and October 4, 2018, DANFORTH received Zelle payments, \$1,000 each transaction, from “Aaron Northern.”

86. On or about September 20, 2018, the Northern Bank-3 Account made three debit card purchases to the Square account of “Shawn Dansforth” in the approximate amounts of \$2,000, \$1,000, and \$500.

87. In or around early January 2019, DANFORTH, using the Moneyy Marley Account, messaged with Mule 4 on Facebook in furtherance of the scheme. User Moneyy Marley sent Mule 4 links to a Bank-10 online bank account. The two exchanged further messages as follows:

Mule 4: light bet  
Moneyy Marley: Hearddddddd  
Mule 4: I did it  
Mule 4: Bro ??  
Moneyy Marley: Yeaaaa  
Moneyy Marley: My fault bro  
Moneyy Marley: Yeaaaaaa just gotta wait 6 days for it to come in the mail  
Moneyy Marley: Soon as that come hit me ( :  
\* \* \* \*  
Moneyy Marley: Just I only Can do it once  
Moneyy Marley: So you gone have to find somebody m  
Moneyy Marley: Else after and get pc lol  
Mule 4: light for how much  
Moneyy Marley: Ima go for like 7  
Moneyy Marley: 2500-3k ya way  
Mule 4: light how I take it out

88. The two users continued the conversation, with user Moneyy Marley instructing Mule 4 that it would take three days to get all of the “bread,” and suggesting that Mule 4 “round some heads,” which appears to mean recruit others to further engage in the fraud scheme.

89. In addition, the Moneyy Marley Account also “hearted” the post containing the Bank-5 Photo posted by the Wallace Account.

90. As discussed further below, it also appears that defendant STEPHANIE LEE SANCHEZ (“SANCHEZ”) allowed her Bank-8 account to be used to send DANFORTH electronic transfers of illegally obtained funds.

### **STEPHANIE LEE SANCHEZ**

91. Based on the investigation, it appears that SANCHEZ allowed a stolen and altered check to be deposited into her Bank-8 account (the “Sanchez Bank-8 Account”) and permitted transfers of the illegally obtained funds to other coconspirators.

92. SANCHEZ maintained the Sanchez Bank-8 Account and, from the account’s inception in May 2018 through December 31, 2018, the account received regular direct deposits from a retail store (consistent with paychecks for employment) and appears to have been tied for payment to a Lyft account. The account also used Square to send and receive money through the account.

- a. On or about September 4 and 7, 2018, two Square transfers from username “StephanieLee” were deposited into the Sanchez Bank-8 Account from a debit card ending in 180, which appears to have been an older debit card issued and used for the Sanchez Bank-8 Account.
- b. On or about September 27, 2018, Square user StephanieLee made another transfer into the Sanchez Bank-8 Account, with a debit card ending in 277, which appears to be a debit card that was issued and used for the Sanchez Bank-8 Account starting around the end of September 2018.

93. After December 31, 2018, nearly all activity on the Sanchez Bank-8 Account ceased until February 8, 2019, including the direct deposits from the likely retail employer described above and the charges from Lyft.

94. Surveillance footage reflects that on or about February 8, 2019, a woman who appears to be defendant SIMONE CORDERO (“CORDERO”) entered a Bank-8 branch in Union, New Jersey and deposited into SANCHEZ’s Bank-8 account a check that appeared to be payable to SANCHEZ in the amount of \$55,000 drawn on Bank-6 from the account of Individual Victim-5, referenced above.

95. According to Individual Victim-5, he/she placed the above-mentioned check in his/her mailbox, and the original intended recipient of the check was the

U.S. Treasury.

96. On or about February 20, 2019, February 21, 2019, and February 22, 2019, a payment of approximately \$1,000 per date was transferred via Zelle from the Sanchez Bank-8 Account to PIERRE's Bank-11 business bank account for "Feed Da Wolves Entertainment, LLC."

97. On or about February 21, 2019, SANCHEZ's debit card ending in 277 was used to check the balance of SANCHEZ's Bank-8 account and conduct four ATM withdrawals in the approximate amount of \$1,000 each at three different ATMs in the Bronx. I know from my training and experience that, in order to effectuate a cash withdrawal from an ATM, the user must both insert a debit card into the ATM and must also type in the personal identification number ("PIN") associated with the debit card.

98. Surveillance footage depicts that on or about February 22, 2019, the same woman who presented the \$55,000 stolen and altered check to be deposited into SANCHEZ's account, who appears to be CORDERO, walked into a Bank-8 branch in Union, New Jersey and made a counter withdrawal of approximately \$5,000 from SANCHEZ's Bank-8 account. The withdrawal slip reflects that the woman presented the bank teller with an identification card bearing a number ending in 713.

99. Records from New York reflect that in or around 2014, SANCHEZ was issued a state identification card with the same number ending in 713.

100. On or about February 21, 2019, February 22, 2019, February 23, 2019, Cash App transfers were made from SANCHEZ's Bank-8 account via her 227 debit card to PIERRE. According to records from Square, these transfers were made in the username of "StephanieLee."

101. On or about February 25, 2019, three ATM withdrawals were made with SANCHEZ's debit card ending in 277 in New York City and the Bronx.

102. According to Bank-8, a Bank-8 investigator contacted SANCHEZ on or about February 26, 2019 about the suspicious activity on her account. SANCHEZ directed the investigator to "go f\*ck herself," and told the investigator that she had lost her debit card and her cell phone. SANCHEZ never filled out paperwork to close, or report fraud for, the account.

103. On or about February 27, 2019, SANCHEZ obtained a New York driver's license.

104. In or around June 2019, law enforcement called, and spoke to, SANCHEZ about her Sanchez Bank-8 Account. SANCHEZ claimed that she lost her wallet, which contained her debit card, her state identification card, and a Medicaid card. SANCHEZ told law enforcement further that she did not open any other bank accounts and did not have an active bank account with any other bank.

105. According to the New York DMV, SANCHEZ never reported that her state identification card had been lost or stolen.

106. Based on the above and the investigation, law enforcement believes that SANCHEZ provided her state identification card, her debit card ending in 277, and the PIN to withdraw money from the Sanchez Bank-8 Account using the debit card, to coconspirators in furtherance of the fraudulent scheme described herein. Law enforcement believes further that SANCHEZ conspired with others regarding the timing of the counter deposit and withdrawals from the account, the CashApp payments, and when SANCHEZ would obtain a new driver's license.

### **SIMONE CORDERO**

107. As discussed above, DANFORTH communicated with Mule 4 in furtherance of the fraud scheme discussed herein on Facebook.

108. On or about March 18, 2020, a post uploaded to Mule 4's Facebook account contained a screenshot of a press release issued by the U.S. Department of Justice regarding charges brought by the U.S. Attorney's Office for the Southern District of New York against, inter alia, Mule 4, CORDERO, and others in connection with federal crimes.

109. CORDERO appeared to have maintained a Facebook account with which the Wallace Facebook account has interacted.

110. An arrest photo taken of CORDERO revealed that CORDERO was the woman described above depositing a stolen, altered check and then, withdrawing cash from SANCHEZ's account while using SANCHEZ's New York State identification card.

111. On or about November 5, 2019, a check drawn on Bank-1 was deposited into a bank account and bore the name "Simone Cordero." According to the individual who originally wrote the check ("Individual Victim-9"), the check was placed in a mailbox in Newark, New Jersey and CORDERO was not the intended recipient and the amount of the check had been altered from \$25 to approximately \$8,326.12. The face of the check bore an address in New Jersey.

### **HANS PIERRE**

112. The investigation has revealed that PIERRE has deposited stolen and altered checks, as well as counterfeit checks, into bank accounts, and has received money transfers from his coconspirators in furtherance of the scheme.

113. Records reflect that the funds that Mule 1 sent via electronic

payments to PIERRE were derived from the stolen altered checks that were fraudulently deposited into Mule 1's bank account. From on or about September 8, 2018 to October 19, 2018, Mule 1 sent 11 successful Cash App payments to PIERRE totaling approximately \$12,000.

114. On or about October 18, 2018, PIERRE performed a song called "CashApp," which was recorded and posted on YouTube. In the song, Pierre declared: "Send the money to my mother f\*cking Cash App."

115. According to records received from Facebook, in or around July 2019, the hustlehans Account on Instagram, believed to be controlled by PIERRE, exchanged messages with the sasuforver Account, believed to be controlled by ADJAVON. The exchange was as follows:

hustlehans: Yoo  
hustlehans: I have a [Bank-7 abbreviation]  
hustlehans: Hit me  
hustlehans: Biz  
sasuforever: Now we talking  
sasuforever: Ok  
hustlehans: Yooo  
hustlehans: You got the work ready  
sasuforever: Not yet  
sasuforever: Will have it tho

116. Thereafter, on or about July 14, 2019, the sasuforever Account messaged hustlehans: "U got the yards?" A minute later, hustlehans responded, "Gathering them now."

117. On or about July 16, 2019, hustlehans sent sasuforever a screenshot. The screenshot contained what appears to be an online username, password, first and last name, and address in New York. As discussed above, through the course of the investigation it appears that members of the conspiracy shared their online banking accounts and/or debit cards with other coconspirators to further the scheme.

118. User hustlehans then sent sasuforever the messages: "You got the yard?;" and "Waitin on the other." User sasuforever replied: "What yard?;" and "U mean food?" User hustlehans responded back: "Info i sent" and with an abbreviated reference to Bank-9. User sasuforever responded: "Yea I got it;" and "Waiting for the food," to which hustlehans responded, "Bet."

119. On or about August 12, 2019, hustlehans and sasuforever exchanged the following messages via Instagram:

hustlehans: It's gon hit  
 sasuforever: Call u soon  
 sasuforever: 20  
 hustlehans: How much could we drop  
 sasuforever: We do it tomorrow  
 sasuforever: It's lit then  
 sasuforever: Ok  
 sasuforever: Phone soon die  
 sasuforever: Hurry  
 hustlehans: I got my own biz  
 sasuforever: Yea

120. On or about August 13, 2019, two checks from two different accounts at Bank-1, both of which bore New Jersey addresses on the face of the checks, were deposited into a Bank-7 business account for "Feed Da Wolves Entertainment," an account controlled by PIERRE. Both checks were reported altered and stolen. One check was written payable to Feed Da Wolves in the amount of \$4,500; the other was made payable to Hans Pierre or Feed Da Wolves in the amount of \$6,500.

121. On or about August 22, 2019, two separate withdrawals from the Feed Da Wolves bank account were made, in the amounts of \$4,000 and \$6,500. Surveillance footage from one of the withdrawals depicts PIERRE entering a bank branch to make the withdrawal.

122. In or around August 2019, hustlehans and sasuforever exchanged the following messages:

hustlehans: Bro  
 hustlehans: Personal [bank name] is good?  
 sasuforever: We could try it  
 hustlehans: Bet  
 hustlehans: Lmk when you want it  
 sasuforever: Ok  
 sasuforever: Gon be like next week  
 hustlehans: Aight

123. Thereafter, on or about August 26, 2019, the hustlehans Account and the sasuforever Account had the following exchange:

hustlehans: Yoo

hustlehans: We make a drop tomw?  
sasuforever: Yup  
sasuforever: Yoyo  
hustlehans: Yooo  
sasuforever: Ya shit still good?  
hustlehans: Yea  
sasuforever: Ight bet  
sasuforever: Gon have to link me today  
sasuforever: How much u wanna do?  
hustlehans: 8  
sasuforever: Bet

124. On or about August 27, 2019, two checks totaling approximately \$7,871 were deposited into a Bank-7 business bank account in the name of “FEED DA WOLVES ENTERTAINMENT, LLC.” PIERRE is the sole authorized signatory to that account. The deposit consisted of two checks in the amounts of \$3,000 and \$4,871, both of which appear to have been drawn on a Bank-4 account for the New Jersey branch of a non-profit network of college-preparatory, free, public charter schools that operates in traditionally educationally underserved communities (“Victim Academy-1”).

125. On or about August 30, 2019, several withdrawals were made from the FEED DA WOLVES ENTERTAINMENT, LLC Bank-7 business account, including a withdrawal of \$3,000 and a withdrawal of \$4,871.

126. The two checks purportedly drawn on Bank-4 for an account held by Victim Academy-1 were returned unpaid as rejected. According to a representative for Victim Academy-1, around this time period, Victim Academy-1 sent a batch of checks in the mail. Shortly thereafter, several checks purporting to be written on behalf of Victim Academy-1 were fraudulently deposited into other people’s bank accounts.