

A Fraudster Named Honesty



This is an ironic case. A man named **Marco Raquan Honesty** was anything but honest. According to federal prosecutors who unveiled charges against him in Virginia this week. The Washington, D.C. man allegedly orchestrated an array of fraud schemes that attempted to steal over \$850,000 through a variety of methods.

In an FBI affidavit , they detail how Honesty reportedly engaged in everything from pandemic loan fraud to sophisticated "smishing" operations - text message phishing scams designed to steal banking credentials.

Honesty Was A Bank Impersonator

Perhaps, the most brazen of his schemes involved impersonating bank employees over the phone.

Honesty also engaged in "SMS phishing. He would send mass text messages claiming to be from banks, warning customers about suspicious activities. When victims called the provided number, they reached Honesty himself, posing as a bank employee. In one recorded call, he successfully convinced a victim to share their complete debit card information while his brother listened in on another line. "Dummy," Honesty allegedly remarked after hanging up, before using the card at a Texas Roadhouse in Arlington, Virginia.

In one recorded conversation with an incarcerated brother, Honesty reportedly explained his technique: "I'm going to call you and say, 'Hello sir, my name is - whatever I want it to be - yes sir, I'm with Wells Fargo fraud prevention team.'"

Honesty Was A PPP Fraudster

The largest monetary scheme involved exploiting the Paycheck Protection Program, netting over \$509,000 in fraudulent loans. Honesty allegedly created a network of fake businesses with similar names - variations of "Lashes by [Name]" or "Cutz by [Name]." Each application used identical financial figures, claiming exactly \$110,752 in gross income. He reportedly charged co-conspirators \$10,000 per successful application, telling his brother he planned to "strike a milly on they ass" once he perfected the system.

Honesty Was An Auto Loan Fraudster

Perhaps his most brazen scheme involved creating fake driver's licenses and documentation to purchase luxury vehicles. In one case, investigators say he created a Maryland license using a victim's name but a co-conspirator's photo, successfully securing an \$81,260 Ford F-350 before the dealership discovered the fraud.

Honesty Was An Account Takeover Specialist Too

Honesty allegedly mastered what he called "bank drops" - gaining unauthorized access to accounts through social engineering. In recorded conversations, he explained his method: "With the emails that I'm able to log into, I try their bank account information as well...and hopefully that's able to be logged into as well. If all that information checks out, then I'm able to do my job." This scheme targeted both individual and business accounts, with attempted thefts reaching \$16,500 in single transactions.

Honesty Was A Check Fraudster Too

Using information gleaned from legitimate checks, Honesty allegedly created counterfeit versions. He explained to his brother that he looked for businesses still issuing physical

checks rather than using direct deposit: "If I can find somebody that get a company...like they work for Wal-Mart, and they get paid through a check...I can make 20 checks off that junk and get my money from Wal-Mart."



A Raid Revealed His Operation

A September 2023 raid on Honesty's residence revealed the sophisticated nature of his alleged operation. FBI agents discovered 24 cellphones, three laptops, blank Social Security card templates, and a credit card embossing machine.

In recorded prison phone calls with his brother, Honesty allegedly boasted about his schemes, saying he "wakes up every day as if he has a job but what he actually does is 'scam.'"

[Read the Full Complaint](#)

IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

UNITED STATES OF AMERICA

v.

MARCO RAQUAN HONESTY,

Defendant.

Case No. 1:24-MJ-441

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A CRIMINAL COMPLAINT**

I, Durrell Douglas, Special Agent with the Federal Bureau of Investigation (FBI), being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (“FBI”) assigned to a white-collar crime squad at the FBI’s Washington Field Office (“WFO”). I have been a Special Agent with the FBI since 2021. During my employment with the FBI, I have received training and exposure to various skills and techniques to include interviewing and interrogation techniques, arrest procedures, search warrant applications, consensual monitoring, analyzing telephone and electronic pen register and caller identification, financial investigations, and electronic and physical surveillance procedures. I have experience with cases involving various crimes to include aggravated identity theft, conspiracy, financial crimes, fugitives, mail fraud, mail theft, money laundering, bank fraud, mortgage fraud, cryptocurrency, and wire fraud.

PURPOSE OF AFFIDAVIT

2. I make this affidavit in support of a criminal complaint and arrest warrant charging MARCO RAQUAN HONESTY (“**HONESTY**”) with one count of aggravated identity theft, in

violation of 18 U.S.C. § 1028A. Although the complaint alleges just one count, I submit that based on the facts herein, there is also probable cause to believe that **HONESTY** and others committed multiple violations of 18 U.S.C. §§ 1343 (Wire Fraud); 1344 (Bank Fraud); 1349 (Conspiracy to Commit Wire and Bank Fraud); 1028 (Identity Theft); 1028(A) (Aggravated Identity Theft); and 1029 (Access Device Fraud).

3. **HONESTY** is a resident of Washington, D.C., with no known legitimate employment. **HONESTY** has an extensive criminal history, which includes credit card fraud and identity theft charges in Virginia, Washington, D.C., and Maryland since 2020. In or around August 2021, he pleaded guilty to misdemeanor identity theft in Virginia. In or around February 2022, he pleaded guilty to misdemeanor fraud charges in the District of Columbia. In or around July 2022, **HONESTY** pleaded guilty to fraud charges in Worcester County, Maryland.

4. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge regarding this investigation. The facts and information contained in this affidavit are based upon my personal knowledge of the investigation and observations of other officers and agents involved. All other observations were relayed to me or to law enforcement by the persons who made such observations. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only. Unless specifically indicated otherwise, all dates set forth below are on or about the dates indicated, and all amounts or sums are approximate.

STATEMENT OF PROBABLE CAUSE

5. Since approximately February 2022, the FBI has been investigating an extensive conspiracy involving multiple fraud schemes and the laundering of the proceeds of those schemes. In general, **HONESTY** plays a central, coordinating role in most of the schemes in which he

participates. In some of these schemes, **HONESTY** directs his co-conspirators to open bank accounts, report fictitious information to bank personnel, and to launder fraud proceeds, often to **HONESTY**'s own financial benefit.

6. In other schemes, **HONESTY** creates fraudulent identification documents, tax documents, and other documents, which **HONESTY** and his co-conspirators use to conduct the fraud schemes described below. More detailed descriptions of some, but not all, of **HONESTY**'s schemes are listed below.

7. **HONESTY**'s brother, D.C., is an inmate in the custody of the Virginia Department of Corrections ("VADOC"). D.C. is incarcerated at the Wallens Ridge State Prison in Big Stone Gap, Virginia, and his expected release date is April 8, 2039. **HONESTY** and D.C. frequently communicate by telephone using the VADOC phone system, which records all non-attorney inmate telephone calls. The VADOC system also notifies participants that it records all non-attorney inmate telephone calls. The FBI has obtained recordings of many of the calls between **HONESTY** and D.C. As described in more detail below, during these calls, **HONESTY** frequently describes or even engages in his fraud schemes.

8. The investigation has revealed that **HONESTY** completes some of the schemes, such as his "smishing" scheme, primarily alone. However, the investigation has also revealed that **HONESTY** conspired with many others to execute other schemes such as the money order scheme and the Paycheck Protection Program scheme.

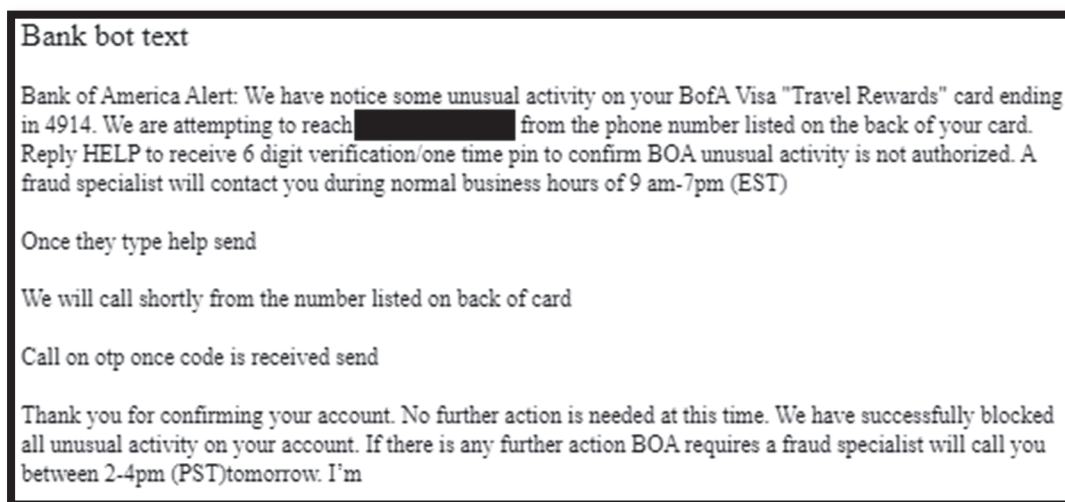
9. On May 13, 2022, the FBI executed a search of **HONESTY**'s Apple iCloud account. The search warrant return yielded text messages, images, and other pieces of evidence described and shown below. On September 7, 2023, a residential search warrant for **HONESTY**'s residence in Washington, D.C. was conducted by the FBI. During the search, multiple devices

including 24 cellphones and 3 laptops were uncovered. A review of these devices yielded additional evidence of **HONESTY** being the perpetrator of various fraudulent schemes.

THE “SMISHING” SCHEME

10. The term “smishing”—short for “SMS phishing”—refers to a scheme whereby fraudsters create and control a website that is spoofed to resemble a legitimate website, such as a bank’s website. The fraudsters then send a short message service (“SMS”) message—also known as a text message—to unwitting victims. Fraudsters craft the text message to appear to be from a bank, and typically a link to a website is included in the message. While the link appears to steer the victim to their bank’s website, it actually takes them to the spoofed website that the fraudster controls.

11. Typically, the fraudulent text message alerts the victim of an unauthorized use of the victim’s funds. If the victim believes the message is actually from their bank, they will often click the link in the text message and enter their username and password into the fraudulent website that the fraudster is monitoring. This allows the fraudster to obtain the victim’s username and password to their bank account. For example, the following is a screenshot of a crafted message labeled “Bank bot text” found within **HONESTY**’s iCloud account:



12. Fraudsters who engage in this type of scheme also usually place a callback phone number in the fraudulent text message they send to their victims. This number is also a spoofed number that typically comes back to a phone controlled by the fraudster. When the victim calls what they believe is their bank, they actually call the fraudster. The fraudster then pretends to be a bank employee to gain access to the victim's information. Fraudsters may use multiple phones or other methods to disguise their true identity in order to engage in communications with fraud victims.

13. On or about January 31, 2022, D.C. used the VADOC phone system to call **HONESTY** on **HONESTY**'s primary phone number. At one point, **HONESTY** asked D.C. if D.C. wanted to hear **HONESTY** "work." **HONESTY** then answered a phone call on a separate phone from an individual identified herein as R.S. In the conversation with R.S., **HONESTY** pretended to be a Citibank employee. Because **HONESTY** engaged in this conversation with R.S. while he was on his primary phone with D.C. (on the VADOC system), the entire conversation was recorded. A transcribed version of the conversation between R.S. and **HONESTY** is below, in relevant part:

HONESTY: *Thank you for banking with Citibank. How may I help you?*

R.S.: *Yes, I just got a text message a little while ago at 12:54. It said something about uh somebody tried to withdraw \$400 out of my account for a Zelle to a Brian Richardson.*

HONESTY: *Yes, there was a Zelle initiated to Brian Richardson from your account. Um, your account is associated with a Citibank phone, with a Citibank account?*

R.S.: *Yes*

HONESTY: *Can I get your name?*

R.S.: *I am [R]. [R.S. spelled his first name] [S].*

D.C.: *How you spell that last name?*

R.S.: [R.S. spelled his last name.]

HONESTY: *Ok give me one second, sir.*

R.S.: *Sure.*

HONESTY (to D.C.): *See how easy that was, bro? Now watch this.*

HONESTY (to R.S.): *Yes sir. Can you verify your billing address for me?*

R.S.: [R.S. gave **HONESTY** his home address in Chicago, IL.]

HONESTY: *Ok give me one second while we look into your account.*

R.S.: *Ok.*

HONESTY (to D.C.): *You hear me, bro? You ready to hear me work? Ready to hear me work work?*

D.C.: *Yes*

HONESTY (to D.C.): *Yeah 'bout to work work. Watch this.*

HONESTY (to R.S.): *Yes sir, I see a someone logged into your account on a Galaxy S6 and sent a Zelle out to a Brian Richardson.*

R.S.: *I don't know who that is.*

HONESTY: *Ok, one second sir. So, you did not send this transaction, correct?*

R.S.: *No I did not.*

HONESTY: *Ok sir, one second while we try to reverse this transaction.*

HONESTY: *Yes sir, can you verify your 16 digit debit card or credit card associated with this account?*

R.S.: *Oh man, let me get my card, let me get my wallet.*

HONESTY (to D.C.): *See how easy that was, bro?*

D.C.: *Yeah*

14. Then, R.S. returned to the line. In the recorded call, R.S. proceeded to give **HONESTY** (posing as a Citibank employee), R.S.'s entire 16-digit debit card number, the expiration date, the three-digit CVV security code, and the last four digits of R.S.'s social security

number. At the close of the conversation with R.S., **HONESTY** stated, “*Yes, yes. I reversed the transaction. We’ll stop the transaction from being sent from Zelle to Brian Richardson. You have a nice day, and if you have any other questions or need anything else, you can give us a call back at the 800 number.*”

15. In reality, no such Zelle transaction had been initiated from R.S.’s Citibank account. **HONESTY** solicited this phone call from R.S. under the false pretense that someone had illegally accessed R.S.’s account and tried to send money from it. **HONESTY** pretended to be a Citibank employee to obtain R.S.’s confidential banking and personal information.

16. When R.S. ended the phone call, **HONESTY**, who was still on the other line with D.C., said to D.C. about R.S., “Fucking dummy.” D.C. and **HONESTY** then laughed at R.S. for about 30 seconds. Later in the call, **HONESTY** said he was “about to go buy me something to eat.” Later that day, R.S.’s Citibank debit card was used at a Texas Roadhouse in Arlington, Virginia—within the Eastern District of Virginia—for \$64.58, thereby overdrafting R.S.’s account. As noted above, R.S. lives in Chicago, Illinois.

17. Later, on the same call between **HONESTY** and D.C., **HONESTY** made the following statements:

HONESTY: *The worst part about it, he didn’t click the link, so I know he don’t have online, so he don’t even have access to know that shit.*

* * *

HONESTY: *Yeah that’s all I do all day bro. Send out, some of them hit the website, some of them call me back. If I can’t get you for your log-in, I’ll get you for your card then!”*

18. The fraudulent activity conducted, and comments made by **HONESTY** are actions recognized as the fraud scheme commonly referred to as “smishing,” as described above.

19. Further, on July 7, 2022, R.S. was interviewed by FBI special agents about the conduct described above. R.S. told the interviewing agents that he believed he was speaking with a Citibank employee and that, if he had known the person with whom he was speaking was not a Citibank employee, he would not have given out any of his information. R.S. did not realize he had been defrauded until he was contacted by the FBI. Accordingly, **HONESTY** was correct in his analysis that R.S. would not be able to detect **HONESTY**'s fraud.

20. The foregoing conduct is the basis of the charge in the criminal complaint. Specifically, on or about January 31, 2022, in the Eastern District of Virginia, **HONESTY** unlawfully possessed, transferred, and used a means of identification of another person, specifically, the debit card information of Victim R.S., during and in relation to the wire fraud smishing scheme, in violation of 18 U.S.C. § 1028A.

THE MONEY ORDER SCHEME

21. From around December 2021 to approximately January 2022, **HONESTY** orchestrated a scheme described herein as the “money order scheme.” To execute this scheme, **HONESTY** and his co-conspirators purchased large quantities of Western Union money orders, typically for \$1.00 each. **HONESTY** and co-conspirators then scratched the true amount off the money order and used computers, software programs, and printers to manipulate the money order to reflect larger amounts, typically \$500.00, \$900.00, or \$1,000.00.

22. Once the amount of the money order was altered, **HONESTY** then deposited the fraudulent money orders into automated teller machines (“ATMs”) at various banks. In some instances, **HONESTY** coordinated with co-conspirators, as described in more detail below, to deposit the money orders and withdraw the proceeds of this fraud scheme. Typically, the banks deposited the amount of money on the fraudulent money orders into the co-conspirators' accounts,

and then the co-conspirators quickly withdrew the cash before the banks could determine that the money orders had been altered and reverse the deposits.

Co-Conspirator 1

23. On or about October 22, 2020, co-conspirator 1 (“CC-1”) opened a Wells Fargo checking account with an account number that ended in x-6868 (“WF 6868”). Records obtained from Wells Fargo show that CC-1 was the sole owner of WF 6868.

24. At approximately 2:49 p.m. on January 5, 2022, five Western Union money orders were deposited into WF 6868. Each of these money orders bore the payment amount of \$1,000.00. Accordingly, Wells Fargo credited CC-1’s account \$5,000.00. Prior to this deposit, WF 6868 had a negative balance of -\$563.20.

25. Text messages recovered from **HONESTY**’s iCloud account revealed a contemporaneous text conversation between CC-1 and **HONESTY** on or about the same day as the deposits. At approximately 2:51 p.m. on January 5, 2022, **HONESTY** sent CC-1 a picture of the receipt associated with the deposit into WF 6868 described above. From approximately 3:04 p.m. on January 5, 2022, to approximately 2:33 a.m. on January 6, 2022, CC-1 and **HONESTY** continued their conversation. A relevant portion of this conversation is transcribed below:

CC-1: *Got it*

HONESTY: [laughing face emoji] *I ain’t playing*

HONESTY: *I’ll be up all night*

CC-1: *I be up tell [sic] 5 every day*

CC-1: *N I got a few ppl for u too*

HONESTY: *Oh shit* [laughing face emoji] *ok*

HONESTY: *Bet bring ‘em especially wells*

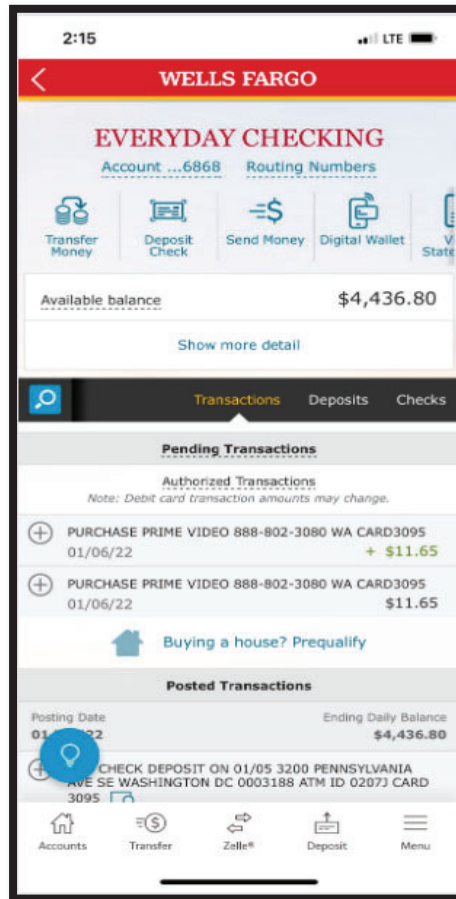
HONESTY: *It’s next day as long as I work before 9pm*

CC-1: *Ok*

CC-1: *2905 30th st SE*

HONESTY: *Send me screenshot of ur account clearing*

26. CC-1 then sent **HONESTY** the following screenshot:



27. The pair continued with the following:

HONESTY: *Bet I'm getting dressed my boy*

CC-1: *We gotta hurry b4 these ppl come n try to get some cash out me n ok me too*

HONESTY: *Bet*

HONESTY: *9 mins*

CC-1: *Ok*

HONESTY: *Outside*

CC-1: *Ok*

28. According to records provided by Wells Fargo, on or about January 6, 2022, \$1,900.00 in cash proceeds of the fraud were withdrawn from WF 6868 in a Wells Fargo bank branch. From January 5, 2022, to January 6, 2022, additional fraud proceeds were withdrawn from WF 6868 via ATM withdrawals and debit card purchases.

29. On or about January 6, 2022, eight Western Union money orders were purchased for \$1.00 each in Alexandria, Virginia. On that same day, the money orders were deposited into WF 6868. Each of these money orders bore the altered payment amount of \$900. Accordingly, Wells Fargo credited CC-1's account \$7,200.00.

30. On or about January 7, 2022, between approximately 2:32 a.m. and 5:25 a.m., CC-1 and **HONESTY** continued their text message conversation, a relevant part of which is shown below:

HONESTY: *How we lookin*

CC-1: *It's there give me an hour tho I just got home from my show I need a shower right quick*

HONESTY: *Bet*

HONESTY: *How we lookin*

CC-1: *It been clear I was tryna get some rest but can't get none fr*

HONESTY: *Wya*

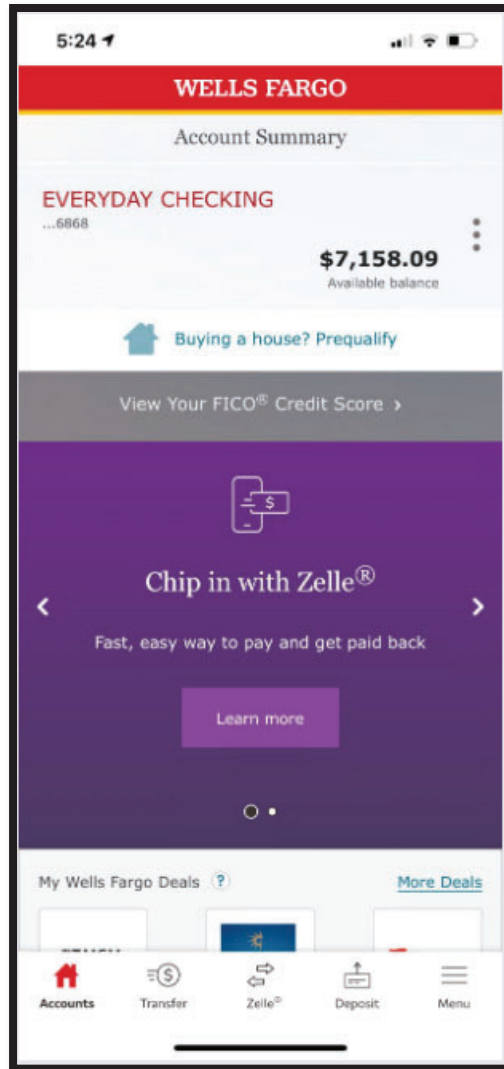
CC-1: *In the house*

HONESTY: *Screenshot me ur account*

HONESTY: *So I can post it but getting clothes on. Ow*

HONESTY: *Now*

CC-1 then sent **HONESTY** the following screenshot:



HONESTY: *I'm loving this shit bruh*

CC-1: *Ik [I know] we goin up*

31. Over the course of approximately January 6 to January 7, 2022, most of these funds were depleted via ATM withdrawals and debit card purchases in the area of Washington, D.C. and Oxon Hill, Maryland. Ultimately, Wells Fargo identified the \$5,000.00 and \$7,200.00 deposits as fraudulent and reversed both of them. Wells Fargo then closed WF 6868 because of the identified fraud. At the time of closing, CC-1's account had an account balance of -\$12,205.31.

32. The text messages exchanged between CC-1 and **HONESTY** coupled with the activity to withdraw funds and make immediate purchases from CC-1's Wells Fargo account shows that the pair conspired together to conduct fraud. Multiple fraudulent money orders were deposited into a Wells Fargo account and then arrangements were made to withdraw the illicit funds via the ATM as soon as possible before the financial institution was able to uncover what occurred and freeze the funds within the account.

Co-Conspirator 2

33. Co-conspirator 2 ("CC-2") is a resident of Roanoke, Virginia. CC-2 and **HONESTY** refer to each other as "cuzzo" in text messages, meaning they are cousins or have some sort of close relationship and association with each other. On or about April 23, 2020, CC-2 opened a Wells Fargo checking account with an account number that ended in x-1022 ("WF 1022"). Records obtained from Wells Fargo show that CC-2 was the sole owner of WF 1022.

34. At approximately 1:55 p.m. on January 10, 2022, D.C. called **HONESTY** on the recorded VADOC phone system. During this call, **HONESTY** told D.C. about his plan to conduct the money order fraud scheme with CC-2. A relevant portion of the call is transcribed below:

HONESTY: *What it do? What it do?*

D.C.: *Chillin, chillin man. Everything alright out there?*

HONESTY: *Yeah about to go out to Roanoke in a minute.*

D.C.: *Oh yeah?*

HONESTY: *Yeah.*

D.C.: *Going to visit the family?*

HONESTY: *Nah I'm going – I'm going to visit family on business.*

D.C.: *Oh.*

HONESTY: *Know I ain't playin. I'm about to go use they ass to make me some money. You know what time it is.*

D.C.: *Hell yeah.*

HONESTY: [CC-2] *got Wells Fargo...about to see nine bands tonight.*

D.C.: *Damn that's what's up.*

HONESTY: *I told you bruh. I don't be playing bruh. I'm real life up off this shit bruh.*

35. The word “band” is slang for \$1,000.00. When **HONESTY** referred to seeing “nine bands,” he was referring to seeing \$9,000.00. Text messages recovered from **HONESTY**'s iCloud account dated January 10, 2022, between 4:21 p.m. and 7:23 p.m., revealed a contemporaneous text conversation between CC-2 and **HONESTY**. This is the same day the call between D.C. and **HONESTY** described above took place. A relevant portion of this conversation is transcribed below:

HONESTY: *Wats ur address*

CC-2: *[STREET ADDRESS] Roanoke Virginia 24013*

HONESTY: *5 mins*

CC-2: *Ok*

36. Later that day at approximately 8:54 p.m. on January 10, eleven Western Union money orders were deposited into WF 1022 at a Wells Fargo ATM in Roanoke, Virginia. Each of these money orders bore the payment amount of \$900.00. Accordingly, Wells Fargo credited CC-2's account \$9,900.00. Prior to this deposit, the balance in WF 1022 was \$549.79.

37. At approximately 4:13 a.m. on January 11, 2022, **HONESTY** texted CC-2 and told her to check her account. CC-2, however, did not respond for approximately seven hours, during which time Wells Fargo identified the \$9,900.00 deposits as fraudulent and froze her account. When CC-2 responded, the following exchange occurred:

CC-2: *Wells called*

HONESTY: *And said.*

CC-2: *I didn't answer I got a email saying they closing my account and blocking deposit*

HONESTY: *Fuckkk*

CC-2: *I know*

* * *

HONESTY: *Wats the move*

CC-2: *We need to find somebody with another bank*

HONESTY: *Bout to pull up on u 15 mins*

HONESTY: *18 waiting on bill*

CC-2: *Ok*

CC-2: *I'm pissed I should've stayed up*

HONESTY: [laughing emoji] *it's cool*

38. Wells Fargo ultimately closed WF 1022. A photo of the receipt for the \$9,900.00 deposit described above was found in **HONESTY's** iCloud account and is captured below. A photo of a Wells Fargo debit card bearing CC-2's name was also found in **HONESTY's** iCloud account.



Co-Conspirator 3

39. On or about October 8, 2019, co-conspirator 3 (“CC-3”) opened a Wells Fargo checking account with an account number ending in x-6593 (“WF 6593”). Records obtained from Wells Fargo show that CC-3 was the sole owner of WF 6593. On or about December 27, 2021, from approximately 4:54 p.m. to approximately 5:00 p.m., eight \$1.00 Western Union money orders were purchased in Alexandria, Virginia, within the Eastern District of Virginia. At approximately 9:48 a.m. on December 29, 2021, four of these Western Union money orders were deposited into WF 6593. Each of the deposited money orders bore the altered payment amount of \$900.00. Accordingly, Wells Fargo credited CC-3’s account \$3,600.00. Prior to this deposit, the balance in WF 6593 was \$154.50.

40. At approximately 1:39 p.m. on December 30, 2021 (i.e., the next day), the remaining four Western Union money orders, which had been purchased in Alexandria, Virginia, were deposited into WF 6593 at an ATM located at 7700 Landover Road, Landover, Maryland. Again, each of these money orders bore the altered payment amount of \$900.00, so Wells Fargo credited CC-3’s account \$3,600.00. Also on December 30, 2021, approximately \$700.00 of fraud proceeds were withdrawn from WF 6593 at the same ATM in Landover, Maryland. From December 29, 2021, to December 31, 2021, approximately \$2,927.00 was withdrawn from WF 6593 via Cash App transactions.

41. About a week later, from approximately 12:09 p.m. to 12:20 p.m. on January 6, 2022, ten \$1.00 Western Union money orders were purchased in Alexandria, Virginia, within the Eastern District of Virginia. At approximately 1:12 p.m. on January 7, 2022, the same ten Western Union money orders were deposited into WF 6593. Once again, each of these money orders bore the altered payment amount of \$900.00, so Wells Fargo credited CC-3’s account \$9,000.00,

bringing the total amount of fraudulent money orders deposited in WF 6593 to \$16,200.00. Photos of the receipts from each of the three deposits were found in HONESTY’s iCloud account and are captured below. Wells Fargo ultimately identified the deposits into WF 6593 as fraudulent and closed CC-3’s account. At the time of closing, CC-3’s account had an account balance of -\$3,599.57.



The ATM Footage

42. The investigation to date has revealed that HONESTY completed the money order scheme with accounts held in the names of at least six other individuals. It is unclear if these individuals cooperated with HONESTY to conduct the scheme with their accounts.

43. For example, on or about December 22, 2021, a checking account was opened at Bank of America in the name of Individual A, ending in x-6825 (“BOA 6825”). Records obtained from Bank of America show that Individual A was the sole owner of BOA 6825.

44. At approximately 3:18 p.m. on January 5, 2022, four Western Union money orders were deposited into BOA 6825 via an ATM deposit. Each of these money orders bore the payment amount of \$900.00, so Bank of America credited \$3,600.00 to BOA 6825. Prior to this fraudulent deposit, no activity had occurred in BOA 6825.

45. Bank of America provided the FBI with the following photo of the individual who deposited the fraudulent money orders into BOA 6825 on January 5, 2022:



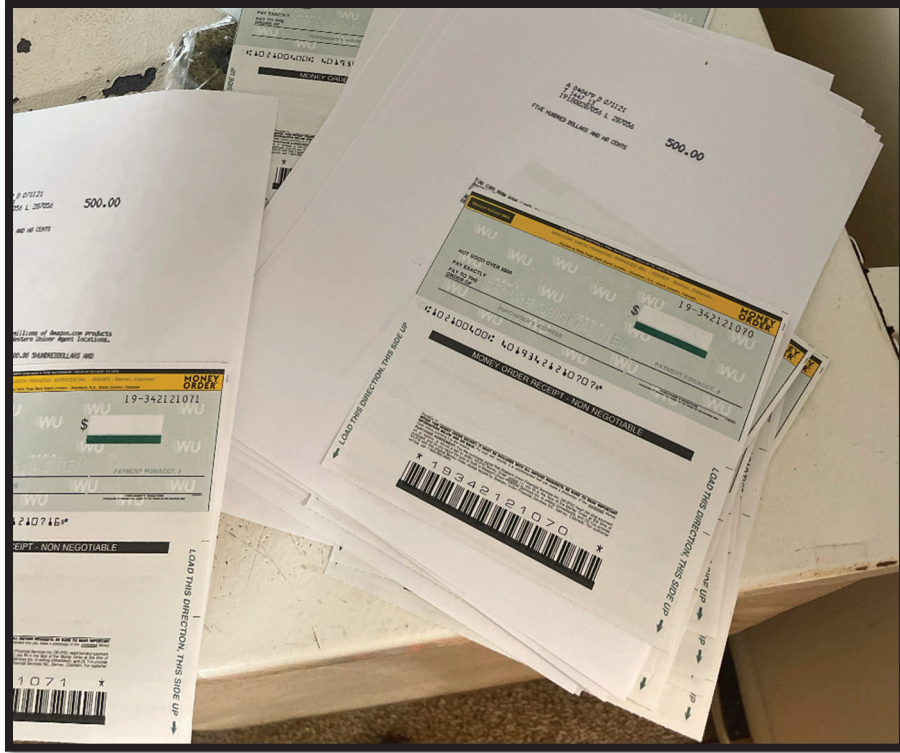
The following photo is a known photo of **HONESTY** from his Instagram account:



46. Based on a comparison of the two photos, it is believed that **HONESTY** was the person who deposited the fraudulent money orders into BOA 6825 on January 5, 2022. Bank of America ultimately identified the deposited money orders as fraudulent and reversed the deposit. A photo of the receipt from this deposit was found in **HONESTY**'s iCloud account.

SUMMARY OF THE MONEY ORDER SCHEME

47. In summary, the investigation to date has determined that **HONESTY** and co-conspirators conspired to deposit at least \$79,700.00 of fraudulent money orders into bank accounts held at Wells Fargo, M&T Bank, and Bank of America. Text messages recovered from **HONESTY**'s iCloud account show that **HONESTY** conspired with CC-1, CC-2, CC-3, and other co-conspirators to conduct this scheme in their respective bank accounts. Multiple photos of receipts for the deposits of these fraudulent money orders were located in **HONESTY**'s iCloud account. The iCloud account also contained multiple photos of loose blank and prefilled Western Union money orders of \$1.00 and \$900.00 with the "Pay To The Order Of" line blank. Text templates for money orders, as shown below, were also located. A review of a laptop belonging to **HONESTY** seized during a residential search warrant conducted by the FBI in September of 2023 also uncovered multiple photos of MoneyGram (money order) templates. These photos show that **HONESTY** was the perpetrator behind the creation of the fraudulent money orders deposited.



(Found in review of iCloud)



(Found in review of laptop)

48. While **HONESTY** was conducting the money order scheme, he engaged in telephone conversations with D.C. in which **HONESTY** updated D.C. about the scheme. For example, on or about January 4, 2022, D.C. called **HONESTY** via the VADOC phone system, and the following conversation occurred:

HONESTY: *I'm on some next level shit...I've been able to make at least like seven, eight bands per bank account...and that shit is real I be clearing literally*

bruh if I drop Monday, it clears 2:30 tonight. If I drop Tuesday, it clears 2:30 Wednesday. If I drop Wednesday, it clears 2:30 Thursday. Like, bruh that shit going crazy.

HONESTY: *I got all cash right now...I'm about to drop three accounts today, so that's going to be 7500 at 2:30 in the morning.*

D.C.: *I'm going to holler at...and try to get some of them junks.*

HONESTY: *Need all them junks bruh. And get them people to re-open they junks. Yeah I need the bank card. Get them to re-open they junks too because that shit was real ass cool...When they sent me that junk, if I would've had work for them it would've been cool. Or if they had even put any money in they account they'd have been good but they closed their account because they ain't put no money in. But they can always go re-open them junks. I went to put something in they account, and the junk spit it out, tell me they account wasn't active no more. This was months ago...As long as you can bring me accounts, you gonna eat...them two accounts you brought me, bruh that was ten racks.*

HONESTY: *By the end of this month bruh, I'm going to get like damn near half a mill worth bruh. I need all that shit...especially if it's going the way it's going.*

D.C.: *Yeah I'm going to start reaching out and trying to find some people.*

HONESTY: *Hell yeah.*

49. Based on investigative efforts to date, along with training and experience, it is under the belief that the term “junks” **HONESTY** uses during these conversations refers to bank accounts. With the help of D.C. within the fraud scheme in recruiting others to re-open their bank accounts, **HONESTY** explained his anticipation to obtain close to \$500,000.00 by months end.

THE PAYCHECK PROTECTION PROGRAM (“PPP”) SCHEME

50. The investigation has further revealed that **HONESTY** and co-conspirators, discussed below, have submitted numerous fraudulent applications for COVID relief loans, in the names of fictitious sole proprietorships. The typical pattern involves **HONESTY** preparing and submitting the paperwork, using information supplied by the co-conspirator. Then, when the loan

money comes in, **HONESTY** gets a cut. Conversations between **HONESTY** and D.C. revealed that **HONESTY** would typically request a cut in the amount of \$10,000.00 per loan.

51. In response to the economic crisis caused by the novel coronavirus pandemic, in or around March 2020, the United States Congress passed the Coronavirus Aid, Relief, and Economic Security Act, Pub. L. No. 116-136, 134 Stat. 281 (2020) (“CARES Act”). Among other things, the CARES Act made government-guaranteed loans available to qualified small businesses through the Paycheck Protection Program (“PPP”). The purpose of loans issued under the PPP was to enable small businesses suffering from the economic downturn to continue to pay salary or wages to their employees.

52. The proceeds of a PPP loan could be used only for certain specified items, such as payroll costs, mortgage interest payments, rent payments, utility payments, and other items. However, the majority of PPP loan proceeds had to be used for payroll. Further, all information submitted to lenders in support of PPP loan applications had to be true and correct.

53. Loan amounts under the program were calculated based on the number of employees the loan proceeds would support. The loans were limited to \$100,000.00 per employee on an annual basis, and the loans were intended to support businesses’ payroll expenses for 2.5 months. Accordingly, a business with one employee would be limited to a loan of \$20,833.00. One employee with a salary of \$100,000.00 would be paid \$8,333.33 per month. In order to pay that employee for 2.5 months, a sole proprietorship could receive a maximum PPP loan of \$20,833.00.

54. Beginning in or around April 2021, **HONESTY** and multiple co-conspirators—to include CC-3 and CC-2—engaged in a scheme to defraud the SBA and several finance companies through the Paycheck Protection Program. Generally, **HONESTY** and others created fraudulent

documents such as 1040 Schedule C Internal Revenue Service (“IRS”) Forms and then submitted those documents to non-bank lenders like Harvest Small Business Finance (“Harvest”), Benworth Capital (“Benworth”), Fountainhead Small Business Finance (“Fountainhead”), and BSD Capital doing business as Lendistry (“Lendistry”). When **HONESTY** and others applied for these loans, they applied for the maximum allowable amount per the PPP rules.

55. The same numbers were used on the majority of the fraudulent 1040 Schedule C IRS Forms created and submitted. Specifically, for more than 10 co-conspirators, 1040 Schedule Cs were created that reflected gross income of exactly \$110,752.00. Investigative efforts revealed none of these forms had been filed with the IRS. Each form also contained material falsehoods on which lenders and the SBA relied on in order to make lending and loan forgiveness decisions. More detailed analyses of some of the PPP loans associated with this investigation are provided below.

PPP Loan for MARCO HONESTY

56. On or about April 14, 2021, **HONESTY** submitted a PPP loan application to Harvest for a \$20,833.00 PPP loan. **HONESTY** represented to Harvest that he operated a sole proprietorship named “Plots by Marco **HONESTY**.” I have found no online presence indicating “Plots by Marco **HONESTY**” is a real business, and the business address **HONESTY** provided on the PPP loan application is associated with a residential apartment.

57. In support of this application, **HONESTY** provided Harvest with a 2019 1040 Schedule C IRS Form. On this form, **HONESTY** claimed gross sales of \$135,940.00 returns and allowances of \$25,188.00, and gross income of \$110,752.00.

58. **HONESTY** submitted this application from the internet protocol (“IP”) address 108.31.51.133, which was assigned to co-conspirator A.F. (hereinafter referred to as “A.F.”), the

mother of **HONESTY**'s children, from February 9, 2021, to April 29, 2021. The investigation has determined that, during the PPP scheme described herein, **HONESTY** and A.F. lived together and were in a romantic relationship. As described in more detail below, **HONESTY** submitted at least five more fraudulent PPP loan applications from this IP address.

59. Based on the information contained in **HONESTY**'s application and the supporting 1040 Schedule C IRS Forms provided, Harvest approved **HONESTY**'s PPP loan application. On or about April 23, 2021, Harvest disbursed \$20,833.00 to the Pentagon Federal Credit Union savings account that **HONESTY** had previously provided to Harvest during the application process. **HONESTY**'s Pentagon Federal Credit Union savings account had an account number that ended in x-1018 ("PENFED 1018").

60. From April 23, 2021, to May 20, 2021, **HONESTY** withdrew \$10,000.00 from PENFED 1018 via in-person withdrawals at Pentagon Federal Credit Union locations. During that same date range, **HONESTY** transferred \$13,980.53 from PENFED 1018 to his checking account ending in x-4021 ("PENFED 4021"). These transfers created a negative balance in PENFED 1018.

61. **HONESTY** subsequently applied to Harvest for a second draw PPP loan based on the application information and documents he had previously submitted. Once again, Harvest approved **HONESTY**'s application and on May 26, 2021, Harvest disbursed \$20,833.00 to PENFED 1018. Before the second disbursement, PENFED 1018 had a negative balance of \$3,881.34. From May 26, 2021, to June 2, 2021, **HONESTY** withdrew most of this money in cash via in-person withdrawals at Pentagon Federal Credit Union locations.

62. Both deposits of **HONESTY**'s PPP loan proceeds into PENFED 1018 were transmitted through PenFed's servers in Chantilly, Virginia.

63. On October 16, 2021, **HONESTY** applied to the SBA for loan forgiveness of his PPP loans. On October 20, 2021, the SBA approved **HONESTY**'s application for forgiveness. In doing so, the SBA assumed all liability for **HONESTY**'s PPP loans.

64. On September 7, 2023, the FBI interviewed **HONESTY** concerning "Plots by Marco **HONESTY**" and the PPP loans the company received. **HONESTY** confirmed he was the owner of the company and explained "Plots" stood for "Phones, Laptops, and Other Tech Systems." **HONESTY** also confirmed that he applied for the PPP loans and claimed the loans received by the company were legit.

65. In addition to applying for fraudulent PPP loans in his own name, **HONESTY** submitted several fraudulent applications in the names of his co-conspirators. **HONESTY** required his co-conspirators to pay him a kickback once they received the proceeds of the fraud. **HONESTY** described this scheme to D.C. during several recorded phone conversations. For example, on or about April 9, 2021, the following conversation occurred:

HONESTY: *Oh bro! Guess what bruh.*

D.C.: *What happened?*

HONESTY: *Bruh they got a new wave come up...it start off at 20 racks, right?*

D.C.: *Yeah*

HONESTY: *It goes to 220*

* * *

D.C.: *Dang*

HONESTY: *Remember that Cali wave that I told you everybody got rich off of?*

D.C.: *Yeah*

HONESTY: *It's back ok? But it ain't Cali no more.*

D.C.: *Oh yeah?*

HONESTY: *Yeah, [co-conspirator M.C.H.] just –*

D.C.: *Did you sign up for it?*

HONESTY: *Did I sign up for it?*

D.C.: *Yeah*

HONESTY: *You damn right! [co-conspirator M.C.H.] just sent me her information for it.*

D.C.: *Oh that's whats up*

HONESTY: *I told her she gotta go half with me. I'm trying to get her for like 30. She gonna get like 22 - 23,000, but I need like 10. You hear me?*

* * *

HONESTY: *Later on tonight, later on today. Yeah, my mother. It's something called PPP. Payment Protection Plan.*

66. On or about April 16, 2021, the following conversation occurred between

HONESTY and **D.C.**

HONESTY: *You know I just cashed out?*

D.C.: *On what, the titles?¹*

HONESTY: *No...something else. For the same amount of money.*

D.C.: *For real?*

HONESTY: *Yeah*

D.C.: *Damn that's what's up bro.*

HONESTY: *I just cashed out. I just cashed out. My shit will be here in like two days, but I already got paid for my first junk bruh. Twenty bands bruh – just cashed out. About to cash out \$40,000 in like six days, but –*

D.C.: *Damn*

¹ I believe that when D.C. asked if **HONESTY** was talking about “the titles,” he was referring to another one of **HONESTY**'s schemes involving fraudulent vehicle titles.

HONESTY: *I got like – I got like nine of them junks going through bro. So it's 40 times nine. You hear me? I'm going HAM on they ass bro.*

D.C.: *Oh that's what's up. That's what I'm talking about.*

HONESTY: *...no cap bruh, the money already going to my accounts and shit. That shit will be here by May 15th bruh, my mother, I'm gonna be like half a mill.*

D.C.: *Damn right! That's what's up.*

HONESTY: *On God – that shit so sweet right now bruh...I'm about to be at like half...I'm almost there. Close to \$100,000 already.*

D.C.: *That's what's up bro, that's what's up.*

HONESTY: *I'm probably like 20 away from 100.*

D.C.: *That's what I'm talking about.*

67. Then, on or about May 10, 2021, the following conversation occurred between D.C.

and **HONESTY:**

HONESTY: *They cut my money off bruh.*

D.C.: *What you mean?*

HONESTY: *The funds ran out. The government ran out of funds bruh.*

D.C.: *Damn.*

HONESTY: *Remember I was making them crazy stupid amounts of money during the week?*

D.C.: *Yeah.*

HONESTY: *Yeah bruh that shit done now bruh.*

D.C.: *Damn*

HONESTY: *Mad as shit bruh. Running they ass up man. I was going crazy bruh, I was going crazy \$4,000 here \$3,000 there. Dude that shit was goin – my income was like \$30,000 here, \$30,000 here, oh 15 - \$20,000 here. That shit started goin crazy bruh.*

D.C.: *Hell yeah.*

HONESTY: *Man – it's all good. Supposedly if they get enough emails saying, you know what I'm sayin, they gonna have to uh give us more money, you hear me?*

D.C.: *Hell yeah*

HONESTY: *Yeah they gonna have to give us more money.*

D.C.: *Damn.*

HONESTY: *Yeah they gonna have to give us some more money. And then they gonna extend it, so they do that then, you know probably like right before June, that shit will kick back off and [people] will begin scoring again....I'm going crazy this time though. I'll probably drop like 70 of them junks, 80 of them junks, you hear me? I probably strike a milly on they ass. Bruh I ain't even gonna lie to you. As soon as they let me know, I'm gonna strike a milly on they ass.*

D.C.: *Hell yeah.*

68. **HONESTY's** statement about the government running out of money was in reference to the original PPP expiration date of March 31, 2021. However, as **HONESTY** described as a possibility to D.C., on March 30, 2021, Congress passed the PPP Extension Act of 2021, which extended the program to June 30, 2021. **HONESTY's** last statement transcribed above indicates that **HONESTY** was planning to submit many more fraudulent PPP loans as soon as the program was re-opened. When **HONESTY** said "a milly," he was referring to submitting multiple fraudulent PPP loans to acquire \$1,000,000.00.

PPP Loan for CC-2

69. As noted above, CC-2 is believed to be **HONESTY's** cousin. On or about April 17, 2021, a PPP loan application for a \$20,833.00 loan was submitted to Harvest on CC-2's behalf. The loan application documents represented to Harvest that CC-2 operated a sole proprietorship named "Best Lashes by CC-2." I have found no online presence indicating "Best Lashes by CC-2" is a real business, and the business address provided on the PPP loan application is associated with a residence. In fact, according to the Virginia Corporation Commission, on or about February 18, 2021, CC-2 incorporated another company, "Runway Aesthetics LLC," which had the same principal office address listed on the PPP loan application for "Best Lashes by CC-2." The

Virginia Corporation Commission site does not contain any records or information for “Best Lashes by CC-2.” Of note, the loan on behalf of CC-2 was submitted only one day after a loan for another co-conspirator was submitted. That co-conspirator’s loan was purported to be for a sole proprietorship called “Supreme Lashes by [co-conspirator’s name]”, a similar name to CC-2’s company.

70. The loan application included what purported to be a 2019 1040 Schedule C IRS Form. This form claimed that CC-2 had gross sales of \$135,940.00, returns and allowances of \$25,188.00, and gross income of \$110,752.00. Once again, these numbers are identical to those in the 1040 Schedule C Forms that **HONESTY** submitted in support of other co-conspirator PPP loan applications to include his own. In review of **HONESTY**’s iCloud account, which produced documents, information, and text messages between **HONESTY** and CC-2, it has been determined that **HONESTY** prepared and submitted the fraudulent PPP loan application in CC-2’s name. Furthermore, CC-2 was aware of and approved of **HONESTY** doing so.

71. For example, the following text message conversation occurred between **HONESTY** and CC-2 starting on or about April 13, 2021:

CC-2: *Sign me up I tried to call you yesterday*

HONESTY: *U work today*

CC-2: *Yess get off @ 5*

CC-2: *I’m Bout to go on lunch if you want to start it now*

HONESTY: *Make sure u be on and sign ur documents*

HONESTY: *One second*

CC-2: *I signed the documents I’m lyk when I get another email*

HONESTY: *Bet bet*

72. On or about April 22, 2021, CC-2 sent several screenshots of emails regarding her pending PPP loan application to **HONESTY**. CC-2 asked for help throughout the process, and **HONESTY** directed CC-2's actions.

73. Based on the information contained in CC-2's application and the supporting 1040 Schedule C IRS Forms provided, Harvest approved CC-2's PPP loan application. On or about April 27, 2021, Harvest disbursed \$20,833.00 to the Wells Fargo checking account that **HONESTY** had previously provided to Harvest during CC-2's application process. CC-2's Wells Fargo account had an account number that ended in x-1022 ("WF 1022"). This was the same Wells Fargo account CC-2 and **HONESTY** used to perpetrate the money order scheme, described above.

74. On or about April 28, 2021, **HONESTY** and CC-2 exchanged text messages, which are transcribed below in relevant part.

HONESTY: *\$lookatmenow0805 for the 3k*

HONESTY: *Also don't forget send me April bank statements and may bank statements when they post too so can I can get ur other 20,833*

CC-2: *My bank declined it say it exceeded the daily limit I'm about to call and see what's the daily limit*

HONESTY: *Oh yea u gotta call them to unlock it*

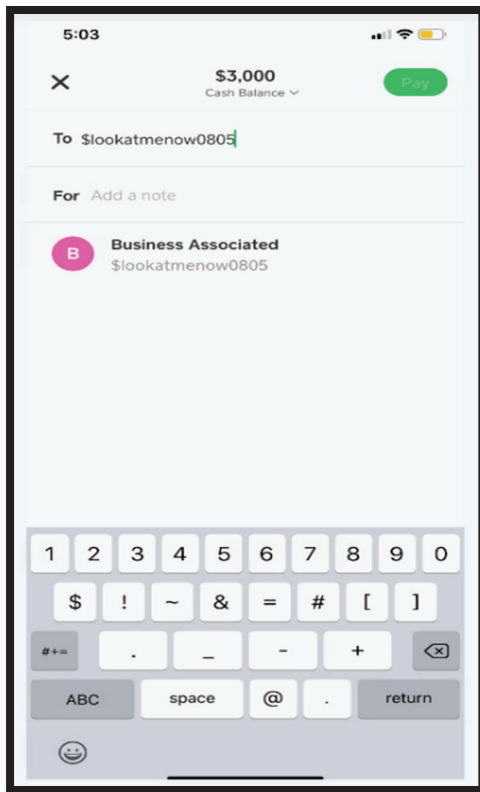
HONESTY: *U unlocked it?*

CC-2: *No my boss on my ass about these cases I'm call on my last break*

HONESTY: *U be busting ur ass at home*

CC-2: *What's your cash app*

CC-2: *This you [CC-2 sent **HONESTY** a screenshot that showed a pending payment to the Cash App username \$lookatmenow0805.]*



HONESTY: *Yea*

CC-2: *You get it*

HONESTY: *Yea I see it it's pending*

HONESTY: *I got it*

CC-2: *Ok*

CC-2: *Thank you cuz and I'm send you more when we do the next one I'm about to get my body done*

75. CC-2 subsequently paid various amounts to plastic and dental surgeons. Based on my training, experience, and knowledge of this case, I believe that when **HONESTY** referred to CC-2's "other 20,833," and when CC-2 referred to the "next one," they were referring to doing a fraudulent second-draw PPP loan in CC-2's name.

76. Records obtained from Block, Inc (Cash App) show Cash App account "\$lookatmenow0805" is registered to **HONESTY**. Records also show this account received

\$3,000.00 from an account with CC-2's first name as the sender on April 28, 2021, the same date the text message conversation concerning payment to Cash App noted above took place.

77. As **HONESTY** and CC-2 had already discussed, on CC-2's behalf, **HONESTY** subsequently applied to Harvest for a second draw PPP loan based on the application information and documents he had previously submitted. On or about May 1, 2021, CC-2 sent **HONESTY** a screenshot that contained an email from the PPP application processing company, Womply, to CC-2. The email stated, in relevant part, "Womply has seen an alarming increase in attempted PPP fraud...We can't emphasize enough that you should not use Womply to commit fraud!" Along with the screenshot, CC-2 asked **HONESTY**, "Did you get this?" **HONESTY** responded to CC-2 and said, "Automated message," and "talking about people using other peoples socials."

78. On May 10, 2021, CC-2 sent **HONESTY** more screenshots of her SBA loan note. CC-2 then said to **HONESTY**, "Cuz I need you to make sure I'm straight I don't want to have to leave my son." This statement by CC-2 shows her awareness of the activity taking place and the possible consequences that could result if caught by law enforcement.

79. Ultimately once again, Harvest approved CC-2's application and on May 12, 2021, Harvest disbursed another \$20,833.00 to WF 1022. Between approximately April 29 and May 28, 2021, CC-2 withdrew over \$29,000.00 of her PPP fraud proceeds in cash, including a \$10,000.00 cash withdrawal from a Wells Fargo bank branch on May 3, 2021. CC-2 also made approximately \$10,515.00 of payments via Cash App and spent over \$3,800.00 at various retail locations.

80. On August 25, 2021, and October 11, 2021, applications for PPP loan forgiveness were submitted to the SBA for both loans received by CC-2. The SBA ultimately forgave CC-2's PPP loans and assumed her liability of \$41,666.00.

PPP Loan for CC-3

81. On or about April 26, 2021, a PPP loan application for a \$20,833.00 PPP loan was submitted to Harvest on CC-3's behalf. The loan application documents represented to Harvest that CC-3 operated a sole proprietorship named "Likez Da Cuts by [CC-3]." I have found no online presence indicating "Likez Da Cuts by [CC-3]" is a real business, and the business address provided on the PPP loan application is associated with a residence in Washington, D.C.

82. The loan application included what purported to be a 2019 1040 Schedule C IRS Form 1040. This form claimed that CC-3 had gross sales of \$135,940.00, returns and allowances of \$25,188.00, and gross income of \$110,752.00. These numbers are identical to those in the 1040 Schedule C IRS Forms that **HONESTY** submitted in support of many of his other fraudulent PPP loan applications. Additionally, the loan application was submitted from IP Address 108.31.51.133, the same IP address registered to A.F., which **HONESTY** submitted A.F.'s loan, his own, and others from as described above. Based on this information, as well as text messages between **HONESTY** and CC-3 recovered from **HONESTY**'s iCloud account, I believe that **HONESTY** prepared and submitted the fraudulent PPP loan application in CC-3's name, and that CC-3 was aware of and approved of **HONESTY** doing so.

83. Based on the information contained in CC-3's application and supporting 1040 Schedule C IRS Forms, Harvest approved CC-3's PPP loan application. On May 5, 2021, Harvest disbursed \$20,833.00 to the Wells Fargo checking account that **HONESTY** had previously provided to Harvest during the application process. CC-3's Wells Fargo account had an account number that ended in x-6593 ("WF 6593"). Also on May 5, 2021, CC-3 withdrew \$10,000.00 in cash at a Wells Fargo bank branch. This was the same Wells Fargo account CC-3 and **HONESTY** used to perpetrate the money order fraud scheme described above.

84. On CC-3's behalf, **HONESTY** subsequently applied to Harvest for a second draw PPP loan based on the application information and documents he had previously submitted. Once again, Harvest approved CC-3's application and on June 4, 2021, Harvest disbursed \$20,833.00 to WF 6593. On June 4, 2021, a \$10,000.00 cash withdrawal was made at a Wells Fargo bank branch from WF 6593.

85. The text message conversation between **HONESTY** and CC-3 that was identified in **HONESTY**'s iCloud account began on August 16, 2021 (i.e., several months after the fraudulent PPP loan applications were submitted). However, in September 2021, **HONESTY** sent CC-3 a document about loans from a company called NetCredit. CC-3 and **HONESTY** then exchanged the following text messages.

CC-3: *Is there a way to finesse the employment part or only do ppl who got jobs*

HONESTY: *Nahh*

HONESTY: *Employment*

HONESTY: *Self employed don't forget u did ppp*

86. In October 2021, **HONESTY** sent CC-3 a screenshot of his email inbox, with two emails from no-reply@sba.gov circled. **HONESTY** and CC-3 then exchanged the following messages, which are transcribed in relevant part.

CC-3: *What that*

HONESTY: *The forgiveness*

CC-3: *Ohh...the sba part threw me off*

HONESTY: *No more owe 41k*

HONESTY: [**HONESTY** sent a video to CC-3]

CC-3: *Bet what I have to do*

HONESTY: *I sent u video*

CC-3: *Okay bet thank you*

CC-3: [CC-3 sent **HONESTY** a screenshot of an email that indicated her request for loan forgiveness had been submitted to the SBA.]

HONESTY: *Perfect*

87. On October 18, 2021, applications for PPP loan forgiveness were submitted to the SBA for both loans received by CC-3. The SBA ultimately forgave CC-3's PPP loans and assumed her liability of \$41,666.00.

SUMMARY OF THE PPP LOAN SCHEME

88. In summary, **HONESTY** conspired with CC-2, CC-3, and others to submit numerous fraudulent PPP loan applications to various lenders. **HONESTY** prepared and submitted fraudulent applications and tax documents. In some cases, **HONESTY** required kickback payments from his co-conspirators for his activity. A few of the co-conspirators worked with **HONESTY**, using him as a guide, to submit their own loan applications. Some co-conspirators also recruited others for **HONESTY** to partake in the fraudulent scheme.

89. The examples described above details how the scheme generally worked for all co-conspirators involved. The investigation to date has uncovered evidence linking **HONESTY** to every application submitted. This evidence includes text messages with co-conspirators about PPP loans and its process, photos of 1040 Schedule C IRS forms sent to co-conspirators via text message, and prison calls between D.C. and **HONESTY** where **HONESTY** spoke about PPP loans and the applications submitted. As noted above, the majority of PPP loan applications submitted used similar or variations of business names such as "Cutz by [co-conspirator name]" or "Lashes by [co-conspirator name]" and similar gross income numbers on 1040 Schedule C IRS Forms. Many applications were also submitted from similar I.P. Addresses that were associated with **HONESTY**.

90. The investigation to date has revealed that at least 16 first draw and 9 second draw PPP loan applications were submitted and approved. A total of 15 co-conspirators were involved in the fraudulent scheme which resulted in a total loss of \$509,069.00 to the SBA.

THE AUTO LOAN FRAUD SCHEME & FAKE IDs

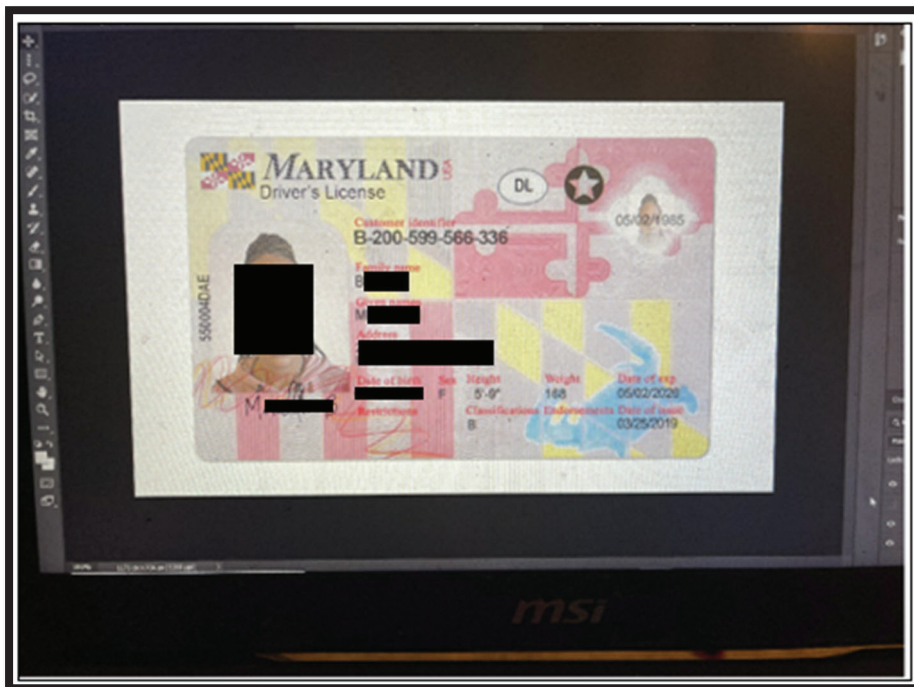
91. As noted above, in one of the phone calls between **HONESTY** and D.C., D.C. asked **HONESTY** about a fraud scheme involving “titles.” A review of the data in **HONESTY**’s iCloud account revealed what is believed to be another scheme to defraud car dealerships by providing fraudulent identification documents, cashier’s checks, and insurance documents in support of ostensible car purchases. **HONESTY** and his co-conspirators supplied these fraudulent documents to dealerships and attempt to purchase vehicles with them before the dealership in question can determine that the documents were illegitimate. **HONESTY** and others engaged in this scheme beginning at least in January 2021 and continued through at least June 2021.

92. For example, I reviewed a text message conversation between **HONESTY** and an unidentified co-conspirator (hereinafter referred to as “UCC-1”) that occurred between approximately January 29, 2021, and August 9, 2021. In this conversation, UCC-1 frequently asked **HONESTY** to make fraudulent checks and identification documents.

93. For example, on or about March 1, 2021, UCC-1 texted a photo of a black woman to **HONESTY**, along with a height and weight, and an address in Hyattsville, Maryland. This woman is believed to be another unidentified co-conspirator (hereinafter referred to as “UCC-2”).

94. **HONESTY** used the picture and information provided by UCC-1 and created a fraudulent Maryland driver’s license with that picture and information but used the name of an identified victim (hereinafter referred to as “Victim M.B.”) on the fraudulent driver’s license.

Later, on March 1, 2021, **HONESTY** sent UCC-1 a picture of his computer screen, which showed that he was making the fake license. The picture **HONESTY** sent is shown below.



95. Then, on or about March 3, 2021, UCC-1 texted **HONESTY**, “ID?” and “They hitting me for it.” In response, **HONESTY** sent UCC-1 a picture of the finished fraudulent driver’s license. The picture is shown below.



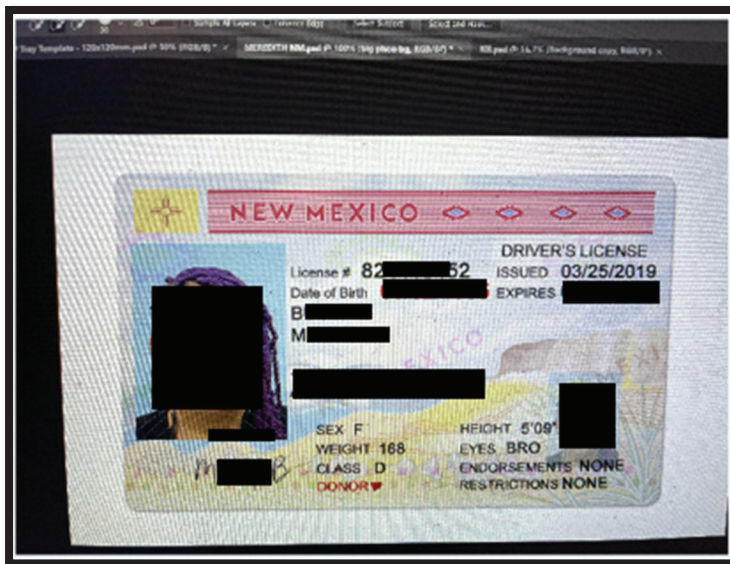
96. **HONESTY** then sent UCC-1 a fraudulent Progressive Insurance card in Victim M.B.'s name.

97. Later in the day on March 3, 2021, UCC-2 went to the Koons Ford of Silver Spring car dealership and purchased a 2021 Ford F-350 Super Duty truck for approximately \$81,260.00. UCC-2 provided the dealership personnel the fraudulent driver's license and insurance card that **HONESTY** previously created and provided to UCC-1.

98. UCC-2 provided dealership personnel with a fraudulent NFCU check for \$15,000.00, which ultimately bounced due to its fraudulent nature. UCC-2 initially secured financing from JP Morgan Chase for the balance of the purchase price.

99. Victim M.B. is an actual person who resides in New Mexico. When M.B. learned of the fraud committed in her name, she disputed the debt with JP Morgan Chase. JP Morgan Chase then canceled the auto loan. However, this process was not completed in time, and UCC-2 successfully stole the vehicle from Koons Ford of Silver Spring. JP Morgan Chase was released from the loan and the car dealership assumed the loss for the vehicle totaling approximately \$81,259.90.

100. Also on March 3, 2021, UCC-1 sent **HONESTY** another picture of UCC-2, albeit with different colored hair. **HONESTY** used that photo to make a fraudulent New Mexico driver's license with UCC-2's photo and Victim M.B.'s information. Approximately 42 minutes after UCC-1 sent **HONESTY** the second photo of UCC-2, **HONESTY** sent UCC-1 a picture of his computer screen, which showed that he was working on a new fraudulent identification. The picture **HONESTY** sent to UCC-1 is shown below.



101. **HONESTY** then sent a message to UCC-1 that said, “Fixed it.” **HONESTY** then sent a picture of the finished fraudulent driver’s license, which is shown below.



102. On or about March 5, 2021, two days after purchasing the Ford F-350 referenced above, UCC-2 posed as Victim M.B. again and used the fraudulent New Mexico driver's license that **HONESTY** made to attempt to purchase a BMW X6 M7 from Passport BMW in Camp Springs, Maryland, at a purchase price of approximately \$126,084.00.

103. The next day, on or about March 6, **HONESTY** sent UCC-1 the personal identifying information and credit card information of an identified victim (hereinafter referred to as “Victim P.H.”). Later that day, Victim P.H.'s JP Morgan Chase credit card was used to make a \$5,000.00 payment to Passport BMW. Ultimately, UCC-2's application for financing through BMW Bank of North America was denied, and the loan was not disbursed. Also, JP Morgan Chase refunded P.H.'s credit card for the \$5,000 paid to Passport BMW as well as other fraudulent charges **HONESTY** conducted.

104. The conversation between UCC-1 and **HONESTY** contains numerous additional victims. Throughout the conversation, UCC-1 asked **HONESTY** to create fake identification documents, checks, and insurance documents. UCC-1 and **HONESTY** often discussed how and when UCC-1 and others would retrieve these items from **HONESTY**. Finally, UCC-1 and **HONESTY** often discussed how much UCC-1 would pay **HONESTY** for his services.

105. The investigation to date has yielded evidence that **HONESTY** creates fraudulent IDs and sells them to others on demand. This evidence includes, but is not limited to, text messages of sales, photos of IDs created sent via text message, multiple headshot photos of individuals located in **HONESTY**'s iCloud account, and photos of **HONESTY**'s computer screen while creating the ID. FBI's residential search warrant executed in September of 2023 referenced above uncovered Real-ID license template logos (pictured below) and electronic devices that contained additional photos and information for the creation of fraudulent IDs.



THE FRAUDULENT CHECK SCHEME & TELEGRAM

106. Telegram is a Dubai-based encrypted messaging application on which users “can send messages, photos, videos, and files of any type (doc, zip, mp3, etc), as well as create groups for up to 200,000 people or channels for broadcasting to unlimited audiences.” Telegram channel owners often create channels that are focused on specific topics for the purposes of posting content and facilitating conversations about the relevant topic. Telegram users are often identified by their Telegram username, which begins with the “@” symbol.²

107. Operators of Telegram channels are able to post content for others to view. Telegram users are able to interact directly with channel operators on their postings, as well as through direct messages, which are commonly referred to as "DMs." Further, "all Telegram chats and group chats are private amongst their participants. [Telegram does] not process any requests related to them."³ Based on my training and experience, white-collar criminals in the United States often use Telegram in their fraud schemes because Telegram is not a domestic company and

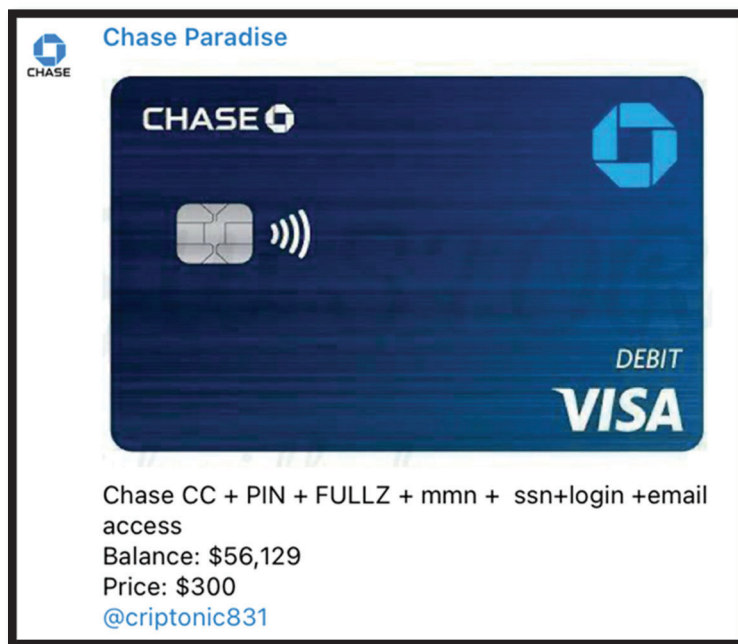
² <https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here> (last accessed September 21, 2022) (emphasis in original).

³ <https://telegram.org/faq> as of September 21, 2022

therefore does not process legal requests for content. Criminals therefore use Telegram to obfuscate law enforcement efforts.

108. Law enforcement has identified two Telegram channels believed to be operated by **HONESTY**; the names of the channels are “Heavenly Logs” and “Chase Paradise.” On the two channels, the operator advertises stolen credit cards, stolen checks, stolen bank log-in information, and other fraud-related contraband for sale to his followers. Based on its content, “Heavenly Logs” refers to stolen bank log-in information that users can purchase from the Telegram channel while “Chase Paradise” refers to stolen credit card information, primarily from JP Morgan Chase, that users could purchase from **HONESTY**.

109. The operator of “Heavenly Logs” typically posts under the username @criptonic831, and the operator of “Chase Paradise” typically posts under the username @godsgoodd. On at least one occasion, however, one of the posts in “Chase Paradise” directed audience members to contact @criptonic831 to purchase stolen credit card information, as shown below:



110. Additionally, the operator of “Heavenly Logs” posted a video to the channel in which the person recording the video shows his hand holding a large quantity of cash and discusses the cash he has. This video captured the person’s distinctive sneakers, as shown below:



111. On at least one occasion, the operator of “Chase Paradise” posted that he was in a U.S. Postal Service (“USPS”) office sending an “order” out. Based on the content of this channel, this post referred to mailing stolen checks to co-conspirators. The operator of “Chase Paradise” also posted a picture of a USPS receipt while standing in a USPS office. This photo, which is shown below, also captured the operator’s shoes:



112. Based on the use of the username @criptonic831 on both Telegram channels, and the distinctive gray and white sneakers that appear in videos on both Telegram channels, I believe that the operator of the “Heavenly Logs” channel and the “Chase Paradise” channel are the same person. Furthermore, I believe that the person who operates both channels is **HONESTY**.

113. First, over the course of this investigation, I have listened to at least 184 prison calls between D.C. and **HONESTY**. Based on my familiarity with **HONESTY**’s voice, I believe that **HONESTY** was the person speaking in the video posted in “Heavenly Logs,” referenced above.

114. Additionally, **HONESTY** and D.C. have discussed **HONESTY**’s use of Telegram on several recorded phone calls. For example, on or about May 21, 2021, in a call between D.C. and **HONESTY** on the recorded VADOC phone system, **HONESTY** told D.C. that he was configuring his new computer. While apparently typing his password on his new computer, **HONESTY** said, “Criptonic831 – my password and save my log-in info, so I can log in whenever

I want. Booyah – back in.” As noted above, the Telegram username that posts frequently in “Heavenly Logs” is @criptonic831.

115. On or about May 2, 2022, **HONESTY** and D.C. had the following conversation on the recorded VADOC phone system, which is transcribed below in relevant part.

HONESTY: *I'm already selling shit on Telegram...*

D.C.: *You said Telegram?*

HONESTY: *Yeah*

D.C.: *What's that? Like a phone network?*

HONESTY: *Nah. Uh, it's where my store at.*

116. Lastly, on or about October 5, 2022, D.C. called **HONESTY** on the recorded VADOC phone system. **HONESTY** told D.C. that he broke his ankle when he jumped a gate while running away from someone.

HONESTY: *I got a cast on my ankle fool.*

D.C.: *Huh?*

HONESTY: *I got a cast on my ankle.*

D.C.: *A cast?*

HONESTY: *Yeah.*

D.C.: *What happened?*

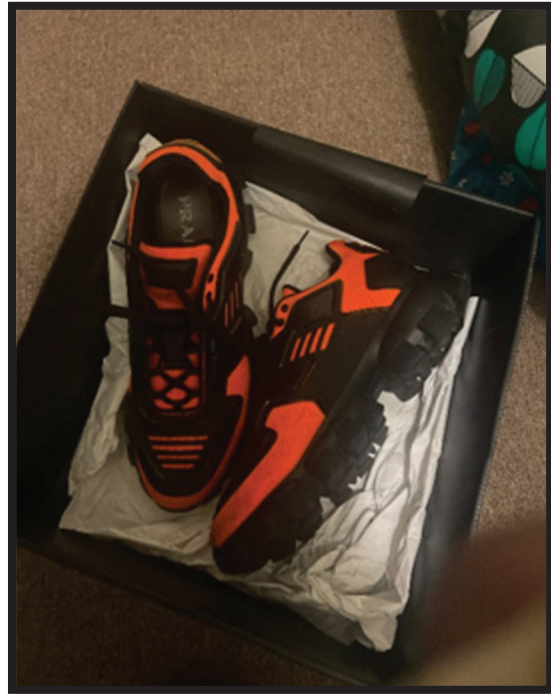
HONESTY: *I broke my ankle.*

117. On or around November 2022, the below photo was posted on Telegram under the “Heavenly Logs” channel. The photo shows a black male with dreadlocks wearing a shoe on one foot and a cast on the other. This photo shows a strong physical resemblance to **HONESTY** based on photos gathered from **HONESTY**'s iCloud search warrant return. Photos of the orange and

black colored shoes worn by the individual pictured in this photo were also found in **HONESTY**'s iCloud search warrant return and during the residential search warrant of **HONESTY**'s residence conducted by the FBI in September of 2023. Photos of the shoes found are pictured below.



(Found in Review of Telegram Account)



(Found in review of iCloud Account)

118. A review of **HONESTY**'s iCloud account data revealed dozens of images of checks believed to be stolen and/or altered to be used in furtherance of **HONESTY**'s and his co-conspirators' fraud schemes. Some of these checks were simply stored on **HONESTY**'s iCloud account, while **HONESTY** sent images of other checks to co-conspirators and friends in text message conversations.

119. An example of this fraud scheme occurred on or about April 6, 2022, when **HONESTY** sent a picture of a Truist receipt, which showed a deposit of a \$8,650.00 check to a Truist bank account ending in x-5917 ("TRUIST 5917"), to co-conspirator 4 ("CC-4"), who also received a fraudulent PPP loan through **HONESTY**. The same photo was also sent to CC-3 on April 6, 2022. The check was drawn on a Citibank account owned by an identified victim (herein

referred to as “Victim J.W.”) and made payable to “Mario Ollie.” **HONESTY** then sent CC-4 two messages that said, “Instant pay” and, “Gonna drop.”

120. Approximately 14 seconds later, **HONESTY** sent CC-4 a picture of a Chase Bank receipt, which showed a deposit of a \$14,741.64 check to a Chase bank account ending in x-2906 (“CHASE 2906”). This check was also drawn on Victim J.W.’s account and was made payable to “Ikea Patrice Lanham.” **HONESTY** then sent CC-4 a message that said, “Maybe on this gotta catch it.”

121. Truist and Chase Bank, respectively, identified both deposits as fraudulent and did not credit the respective deposit accounts.

122. Another example of this fraud scheme occurred in April 2022 when **HONESTY** and co-conspirator 5 (“CC-5”) worked together to deposit a fraudulent check into CC-5’s Citibank account ending in 7872 (“CITI 7872”). Beginning on or about April 2, 2022, **HONESTY** and CC-5 exchanged the following text messages:

HONESTY: *Oh yea apply for truist bank*

CC-5: *Done*

HONESTY: *And as many banks as u can tbh so [people] can be loaded*

CC-5: *I got u*

HONESTY: *Chase, td, boa again , industrial bank it’s a new one I seen pop up but ima do my research got s feeling they sweet*

CC-5: *Ima get the most I can*

CC-5: *Ima see which ones can be done online*

HONESTY: *Bet that*

HONESTY: *Cuz ima touch ur Citibank Monday so....*

CC-5: *With the big one right*

HONESTY: *Nice to fertilize ground so when it's time to plant seeds it's time like this*

HONESTY: *U can use each one for zelle to bring activity then spankem*

CC-5: *Killlllll...*

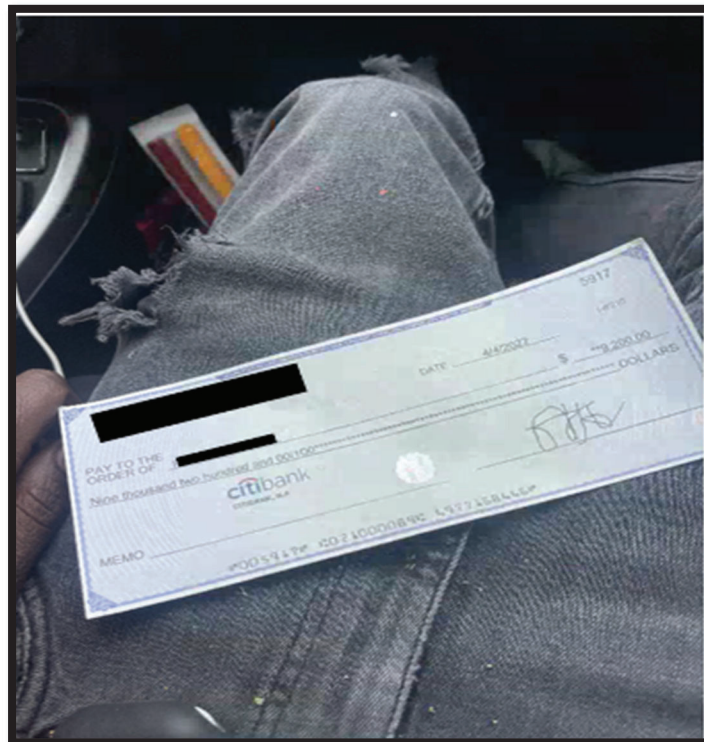
CC-5: *Aye all this zelle bread I'm making getting put up like that cb bread I had*

HONESTY: *Yea but u gonna make more from this*

HONESTY: *Substantially a lot*

CC-5: *Damnnnnnn*

123. On or about April 5, 2022, **HONESTY** sent CC-5 a message that said, "How we looking." Approximately one hour later at approximately 7:55 a.m., **HONESTY** sent CC-5 a picture of a \$9,200.00 fraudulent Citibank check drawn on the account of Victim S.B. and made payable to CC-5. Victim S.B. appears to be a medical doctor in New York. The picture of the check that **HONESTY** sent to CC-5 is shown below.



124. Approximately eight minutes later, **HONESTY** sent CC-5 a screenshot of what I believe to be an internet search for Victim S.B. That screenshot shows that Victim S.B. is a physician in New York. Accordingly, I believe **HONESTY** and CC-5 knew Victim S.B. was a real person when they exchanged these text messages about the check fraud scheme. The screenshot **HONESTY** sent to CC-5 is shown below.



125. According to bank records provided by Citibank, on April 4, 2022, at approximately 1:09 p.m., the fraudulent check described above was deposited into CITI 7872 at an ATM in Washington, D.C. Approximately three hours later, a cash withdrawal of \$900.00 from CITI 7872 was conducted at the same ATM in Washington, D.C. Approximately seven hours later, a cash withdrawal of \$120.00 from CITI 7872 was conducted at an ATM in Alexandria, Virginia, within the Eastern District of Virginia.

126. The next day, on or about April 5, 2022, an ATM withdrawal of \$1,000.00 and an in-person withdrawal of \$5,000.00 were conducted on CITI 7872. On or about April 6, 2022, Citibank identified the fraudulent nature of the check and reversed the transaction.

127. **HONESTY** often discussed his fraudulent check scheme with D.C. on recorded prison phone lines. Some examples of these conversations are transcribed below in relevant part.

August 30, 2021

HONESTY: *It's a bank drop. You know what a bank drop is? You grabbing a fake check and you drop it into a fucking bank and you hope the bank...gives you the money*

D.C.: *Yeah*

HONESTY: *I said first you got to understand how bank drops work.*

D.C.: *Yeah*

HONESTY: *When you get a bank drop, ok, I'm gonna teach you something. Anything under five thousand can clear in one to three days. One to three business days. You listening to me?*

D.C.: *Yeah*

HONESTY: *Anything over five thousand takes three to five business days.*

D.C.: *Ok.*

HONESTY: *Anything over that amount takes up to 10 business days.*

D.C.: *I got you.*

128. Based on my training, experience, and knowledge of this case, I believe that **HONESTY** was explaining to D.C. about how quickly a fraudulent check could be cashed, depending on the amount of the check.

September 4, 2021

D.C.: *The bank junk ain't come through?*

HONESTY: *uh-uh*

D.C.: *Dang*

HONESTY: *But I ain't drop all of them. I only dropped two of them. To see if it was going to click. I seen that they didn't click, so I already know what I needed. I need to find somebody who get paid by a big business who actually gets a physical check because everybody else gets direct deposit that I know of.*

D.C.: *Yeah*

HONESTY: *Pops get direct deposit. Everybody I know with a job gets direct deposit...it don't go through a check. But if I can find somebody that get a company, you know what I'm saying like they work for Wal-Mart, and they get paid through a check*

D.C.: *Yeah*

HONESTY: *Oh yeah, I can use that check to steal from Wal-Mart. I can make 20 checks off that junk and get my money from Wal-Mart.*

D.C.: *Damn*

HONESTY: *Yeah, that's how that shit work. It ain't nothing but [people] intercept checks or my bitch might work for a bomb ass company that's rich as fuck, and she get a check, so what she do is just show me the numbers on a check. Them numbers are registered to that company's account and you know what that mean, it's basically that company's money.*

D.C.: *mh-hmm*

HONESTY: *You don't know how much money in they account but it's basically they money so you can just start signing shit off. See I'm about to make one for six bands [\$6,000] see if this clears – it clears, oh shit! I'm about to try one for eight bands [\$8,000] – oh it clears. I'm about to try one for 14 – oh it clears. I'm about to try one for 10 – oh that junk was dead. Oh damn, damn, we probably stole...through they money...That's how that shit works.*

D.C.: *Yeah*

129. Based on my training, experience, and knowledge of this case, I believe that **HONESTY** was discussing forging checks by copying the routing and account numbers from hard-copy payroll checks that companies send out.

130. **HONESTY** then went on to describe to D.C. another part of his fraudulent check scheme in the same phone conversation, as transcribed in relevant part below.

HONESTY: *Basically somebody might used to live there and they check might come there. What a [person] would do is come to me. I make an ID for that same name that's on that check – they gonna cash that bitch.*

D.C.: *Yeah*

HONESTY: *That's a guarantee. Every time I get one of them, I automatically cash the junk....And now I got my little machine back, oh yeah, it's no stopping me. I just need that work for that cash. And I'm not, again, I'm not bagging a whole trucks and all that. I ain't on that gangster shit like that.*

D.C.: *Yeah*

HONESTY: *I mean, it ain't gangster if you bag a truck, but it's gangster to me because I ain't trying to do that time for that shit.*

D.C.: *Yeah*

HONESTY: *I ain't tryin to have that on my – on no paperwork with no case...armed robbery, fucking you know that's...like federal. That's like, I don't know, that's like trying to rob a police officer or something.*

131. Based on my training, experience, and knowledge of this case, I believe that **HONESTY** was discussing the creation of fraudulent identification documents that **HONESTY**'s co-conspirators could use to cash payroll checks intended for another person. **HONESTY** also discussed his preference for non-violent fraud schemes because he believed they carried shorter prison sentences than violent crimes, such as armed robbery.

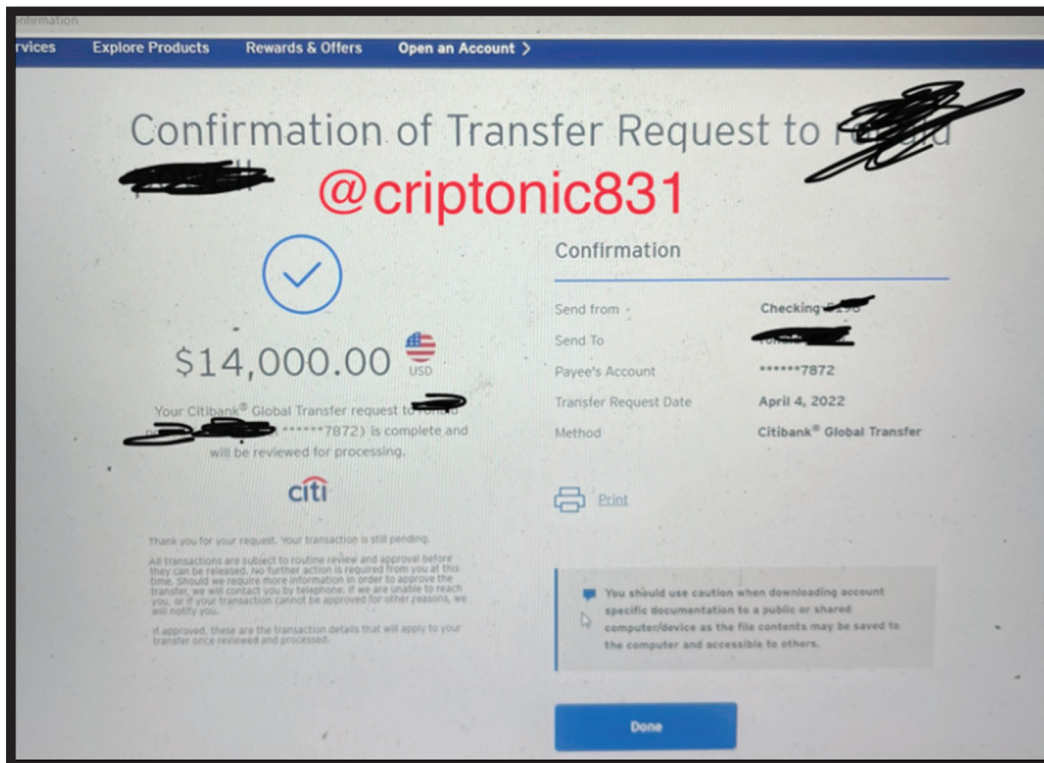
THE ACCOUNT TAKEOVER FRAUD SCHEME

132. **HONESTY** also orchestrated an account takeover scheme whereby he gained access to victim accounts and then, without the knowledge or permission of the account owner, transferred money to himself and his co-conspirators via payment platforms such as Zelle and intrabank transfers, among other means.

133. On or about April 4, 2022, an identified victim (hereinafter referred to as "Victim S.J.") received a text message about fraudulent activity in his Citibank checking account ending in x-5196 ("CITIBANK 5196"). Victim S.J. followed the instructions in the text message he received. Later that same day, approximately \$16,500.00 of completed and attempted transfers

from CITIBANK 5196 were conducted. These funds were transferred (or attempted to be transferred) to accounts maintained by multiple co-conspirators, including CC-4 and CC-5.

134. Also on April 4, 2022, a \$14,000.00 “Citibank Global Transfer” payment was attempted from CITIBANK 5196 to CC-5’s Citibank account ending in x-7872 (“CITIBANK 7872”). During the review of HONESTY’s iCloud account, a screenshot of the attempted transfer posted below was found.



135. The screenshot shows a Citibank Global Transfer confirmation of transfer request. The name of the recipient is mostly redacted, and “@criptonic831” is written in red letters beside the payee’s redacted name. As referenced above, the investigation has determined that @criptonic831 is HONESTY’s username on Telegram.

136. On June 24, 2024, the FBI interviewed Victim S.J. During the interview, Victim S.J. explained that he clicked on the link he received and provided all of the information that he

was asked to provide. Victim S.J. was unaware that he was providing the information to a fraudster. Victim S.J. confirmed the funds were withdrawn from his account via Zelle transfers and the financial loss suffered was approximately \$10,000.00.

137. On or about September 13, 2022, **HONESTY** and D.C. participated in a phone call on the VADOC recorded line. During this call, **HONESTY** described to D.C. how he gains access to victim bank accounts. A relevant portion of this call is transcribed below.

HONESTY: *So, then I'm gonna tell you my job. So, once I load – ok so – there's no point in me performing my job unless I have somewhere to send to. You get me?*

D.C.: *Yeah*

HONESTY: *Now, what I do is I hack/spam, right?*

D.C.: *Yeah*

HONESTY: *So, the way that I'm able to get my money is throughout the day that I spam some – you know what I'm saying – so many text messages that I send, blah blah blah, usually it comes with some people that have certain emails that I'm able to log into. All emails are not loggable into.*

D.C.: *Ok*

* * *

HONESTY: *With the emails that I'm able to log into, I try their bank account information as well...and hopefully that's able to be logged into as well. If all that information checks out, then I'm able to do my job.*

D.C.: *Ok ok.*

HONESTY: *So like last time when I was in Virginia, I ended up doing a spam. Yes, I did get 23 cards, but out of them 23 cards, all of them were Gmails, which are unable to be gotten into.*

D.C.: *Dang*

HONESTY: *You get what I'm saying? I even got shit with fifty thousand, forty thousand able to be transferred, but because they're Gmails, I'm unable to get into them. Now, the other way for me to get into them – if I call and become the banker myself. So I noticed that you are Johnathan Wayne, and you bank*

with Wells Fargo, so I'm going to call you and say, 'Hello sir, my name is - whatever I want it to be – yes sir, I'm with Wells Fargo fraud prevention team, sir yes sir we noticed unusual activity in your account. Sir, we are going to send a six digit verification code to your phone sir we need you to repeat that verification code...in order for us to verify you sir.' Get it?

D.C.: *Yeah*

HONESTY: *Why the fuck did I just call him and say that? Hey it work though. 'Oh what? Unusual activity? What? Yeah yeah send the code.' Ok. 'Yes sir, can you repeat the code?' The code is dah dah dah. 'Thank you sir.' ...Thank you for that code, dummy. I'm in your account...'Alright, yes sir. You verified everything and we stopped the transaction. You may now use your account as normal. Anything else I can help you with today, sir' ...And that's how it works. Now, out of ten calls...six answer. Out of them six calls that answer, two to three give up the code.*

D.C.: *Ok ok.*

FBI RESIDENTIAL SEARCH WARRANT – SEPTEMBER 7, 2023

138. On or about September 7, 2023, the FBI executed a residential search warrant at **HONESTY**'s residence located at 337 17th Street NE, Washington, D.C. 20002. During the search warrant, FBI seized, among other things, the following:

- a. 24 cellphones;
- b. three laptops;
- c. smart watches jewelry;
- d. two handguns and ammunition;
- e. blank Social Security card templates;
- f. one 16-lb box of blank IRS 1099 forms;
- g. Virginia temporary vehicle tags;
- h. multiple SIM cards for cellphones ;
- i. one tan-colored credit card embosser machine;
- j. multiple blank, white cards with microchip;

- k. one black credit card reader;
- l. One debit card in the name of a third party with no apparent relation to **HONESTY**;
- m. One check for \$95.59 from a third party in Silver Spring, MD with no apparent relation to **HONESTY**, made payable to Verizon; and
- n. Approximately five pieces of mail from utility companies and other businesses for address 337 17th Street addressed to third party names with no apparent relation to **HONESTY**.

139. The FBI also located and identified the black and orange tennis shoes found in the picture posted to the Telegram channel and iCloud account, as referenced above, as well as designer watches matching those seen in images posted by the user of the Telegram channel. Additionally, the FBI recovered a silver Alienware laptop seen in videos found in **HONESTY**'s iCloud and on the Telegram channels conducting fraudulent activity.

140. The search warrant obtained for **HONESTY**'s residence also authorized the search of digital devices recovered from his residence. The FBI's review of some of the digital devices seized from **HONESTY**'s residence revealed multiple photos of fraudulent driver's licenses, photos of fraudulent checks being made, templates for Western Union money orders, Paycheck Protection Program documents, and multiple lists of personal identifier information for multiple individuals, to include name, date of birth, and social security numbers.

141. On the same day of the search warrant, **HONESTY** agreed to be interviewed by FBI agents. During the interview, **HONESTY** claimed that his income was earned from completing odd jobs such as moving and landscaping. However, this investigation has not uncovered any legitimate employment by **HONESTY**. To the contrary, in phone calls **HONESTY** made to D.C., **HONESTY** stated that he would not be able to have the things he

owned if he were working a full-time job; he further stated that he wakes up every day as if he has a job but what he actually does is “scam.”

SUMMARY

142. As described above, the investigation to date has revealed that **HONESTY** engaged in multiple fraud schemes, including “smishing,” PPP loan fraud, money order fraud, check fraud, auto loan fraud, and account takeover fraud. While **HONESTY** conducted some of these schemes by himself, he also conspired with others known and unknown to the government to conduct other schemes such as the PPP loan, money order, and auto loan fraud schemes. As previously mentioned, this affidavit does not contain every detail and fact of the investigation to date. The known attempted loss for all fraud schemes combined is \$850,204.64. The actual known loss amount of all fraud schemes is \$621,958.50.


Fraud Scheme	Attempted Loss	Actual Loss
Money Order Scheme	\$79,700.00	\$22,248.79
PPP Loan Scheme	\$509,069.00	\$509,069.00
Auto Loan Scheme	\$212,344.00	\$81,260.00
Check Fraud Scheme	\$32,591.64	\$6,880.71
Account Takeover Scheme	\$16,500.00	\$2,500.00
<u>Total:</u>	\$850,204.64	\$621,958.50

CONCLUSION

143. Based on the forgoing, I submit that there is probable cause to believe that on or about January 31, 2022, Marco Raquan **HONESTY** did knowingly and unlawfully possess, transfer and use, without lawful authority, a means of identification of another person—the debit card information of R.S.—during and in relation to the commission of a felony enumerated in 18 U.S.C. § 1028A(c), to wit, wire fraud in violation of 18 U.S.C. § 1343, knowing that the means of identification belonged to another actual person.

144. I therefore request that the Court issue the proposed criminal complaint and associated arrest warrant.

Respectfully submitted,



Special Agent Durrell Douglas
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on November 4, 2024.



Digitally signed by Ivan Davis
Date: 2024.11.04 14:29:32 -05'00'

Hon. Ivan D. Davis
United States Magistrate Judge