

Bank Employee Used iPhone to Photograph Customer Data, Steal \$327,000



A bank employee in western New York used his iPhone to secretly photograph sensitive customer information from his work computer, then shared those details with accomplices who drained bank accounts of close to 12 victims.

Federal prosecutors say Damani Brown's ten-day crime spree shows how insider threats can quickly turn employee access into major financial losses.

Brown worked as a customer service representative at an unnamed bank when he began his scheme on July 27, 2024. He would look up customer accounts on his work terminal, then use his iPhone 14 Pro to take pictures of the screens showing bank account numbers, social security numbers, and other personal details.

He Left A Digital Paper Trail

FBI agents found the smoking gun evidence in Brown's iCloud account. Photos stored on the Apple platform showed his iPhone displaying bank computer screens with customer lookup pages. One image captured multiple customer records, including details for "Victim Customer 1" according to the criminal complaint filed in federal court.

Brown had a simple way to steal information. He would search a customer's account during his work shift, often when the person wasn't even visiting the bank

branch. Within hours, his partners would register online banking accounts using the stolen information.

His fraud ring partners used Gmail accounts to receive verification codes from the bank.

Once inside the online banking system, they moved money to other accounts at the same bank, then withdrew cash at local branches.

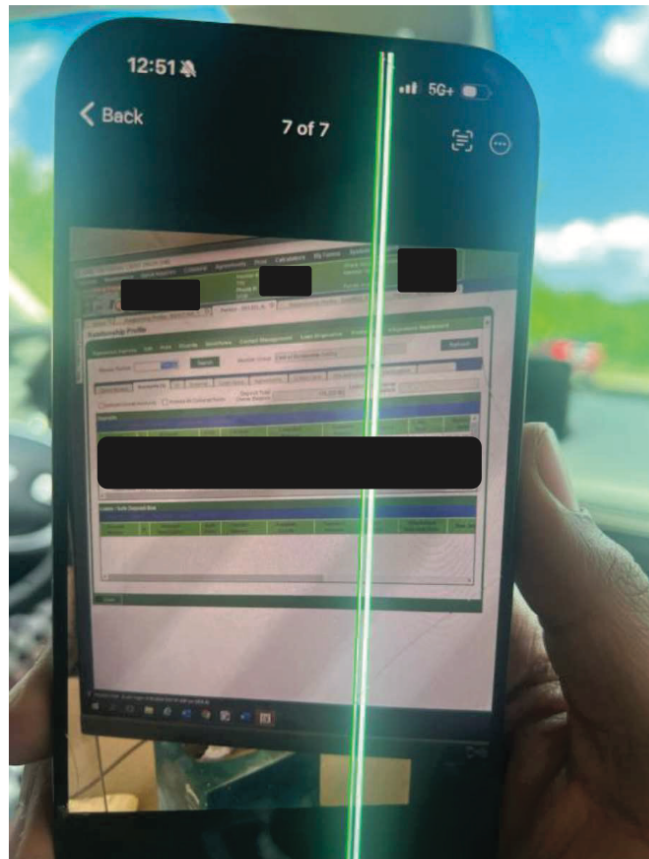
The Accounts He Took Pictures Of Were Drained Fast

There were many victims but the case of "Victim Customer 9" shows how quickly the fraud unfolded.

On July 31, 2024, at 1:45 PM, Brown looked up this customer's account information. The next day, someone registered an online account using the customer's bank member number and social security number.

Phone records show Brown called a number linked to an accomplice three times on August 6.

That same day, the thieves moved \$30,436.70 out of Victim Customer 9's accounts. The victim later told FBI agents they never registered for online banking and never gave anyone permission to access their money.



Investigators Found Telegram Messages

Investigators found Telegram messages on Brown's phone showing how the criminal network operated. In one conversation, someone using the handle "Looch" provided complete personal details for Victim Customer 10, including name, bank account number, social security number, phone number, date of birth, and address.

The messages reveal casual attitudes toward the crimes. "And that's fine we can work around stuff like that we just need new logs," one participant wrote. Another message discussed a customer with "\$41k in a joint account."

They Traced His IP Address And Bank Confirmed Screen Shots Were Real

The FBI traced IP addresses from Charter Communications and T-Mobile back to Browns accomplices. Website cookies linked multiple fake email accounts, showing they were accessed from the same devices and browsers.

Apple provided detailed logs showing when and how the fraudulent accounts were accessed. The same device identifier appeared across multiple suspicious login sessions between May and August 2024.

Bank officials also confirmed that the photos found on Brown's phone matched real customer lookups in their system. The images showed accurate timestamps, terminal locations, and network activity that only Brown had accessed during those specific times.

Over \$477,000 Stolen In 10 Days

Twelve bank customers lost money they didn't know was missing until days later. The thieves transferred approximately \$477,000 total.

The unnamed bank was able to recover some of the funds.

All victims confirmed they never registered for online banking, never allowed anyone else to access their accounts, and never authorized the transfers. Some stolen money went through CashApp before disappearing completely.

The bank's internal review after the incidents revealed Brown's suspicious account lookups. Customer service representatives typically access accounts only when helping people at branch locations or over the phone. Brown's searches happened when none of his victims were seeking assistance.

Smart Phones Present An Internal Fraud Risk

The use of smartphones to photograph computer screens represents a low-tech method for stealing high-value data. Traditional security systems that monitor file downloads or email attachments wouldn't detect someone taking pictures with their personal phone.

Federal Charges and Investigation Is Now Underway

Brown faces six federal charges including conspiracy, aggravated identity theft, access device fraud, computer fraud, and bank fraud. If convicted on all counts, he could face decades in prison.

The criminal complaint filed in the Western District of New York details the FBI's months-long investigation. Special Agent Jordan Slavik's affidavit runs 20 pages and includes screenshots from Brown's devices showing the criminal activity.

Read The Complaint On Following Pages

UNITED STATES DISTRICT COURT

for the

Western District of New York

United States of America

v.

DAMANI BROWN

Case No.

25-MJ-4085

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

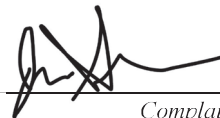
On or about the date(s) of 7/27/24 through 8/6/24 in the county of Monroe in the
Western District of NY, and elsewhere, the defendant(s) violated:

*Code Section**Offense Description*

18 USC 371	Conspiracy
18 USC 1028A	Aggravated Identity Theft
18 USC 1029(a)(2) and (b)(2)	Access Device Fraud and Conspiracy to Commit Access Device Fraud
18 USC 1030(a)(4) and (b)	Computer Fraud and Conspiracy to Commit Computer Fraud
18 USC 1344	Bank Fraud
18 USC 1349	Conspiracy to Commit Bank Fraud

This criminal complaint is based on these facts:


See the attached Affidavit of Jordan F. Slavik, which is incorporated by reference as if set forth fully herein

☒ Continued on the attached sheet.*Complainant's signature*

Jordan F. Slavik, Special Agent, FBI

Printed name and title

submitted electronically by email in .pdf format. Oath administered, and contents and signature attested to me as true and accurate telephonically pursuant to Fed. R. Crim. P. 4.1 and 41(d)(3).

Date: June 24, 2025*Judge's signature*City and state: Rochester, New York

Colleen D. Holland, United States Magistrate Judge

Printed name and title

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

STATE OF NEW YORK)
COUNTY OF MONROE) ss:
CITY OF ROCHESTER)

I, JORDAN F. SLAVIK, 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 and have been so employed since September 2019. I am currently assigned to the Cyber Squad, Buffalo Division, in Rochester, New York, where I work on investigations relating to criminal and national security cyber intrusions. These investigations specifically focus on unlawful computer access, nefarious online marketplaces, phishing activity, and online sexual extortions. I have gained experience through numerous FBI, government, and private sector trainings and certifications such as: multiple certificates through the FBI's Advanced Cyber Training Program and cryptocurrency training curriculum; the Department of Homeland Security's Cybersecurity for Industrial Control Systems certificate; certificates from SANS on Cyber Security essentials, Hacking Tools, and Open Source Cyber Investigations; and certificates from Mandiant on the Cybersecurity Intelligence Cycle, as well as through everyday work related to these types of investigations. Through my work in cyber-related investigations, I am familiar with the fundamental operations of the internet, hardware, and software, and the communication protocols across each. As a Special Agent with the FBI, I am empowered by law to investigate and make arrests for offenses against the United States.

2. As detailed below, I make this affidavit in support of a criminal complaint charging Damani Brown (hereinafter “BROWN”) with violations of Title 18, United States Code, Sections 371 (Conspiracy), 1028A (Aggravated Identity Theft), 1029(a)(2) and (b)(2) (Access Device Fraud and Conspiracy to Commit Access Device Fraud), 1030(a)(4) and (b) (Computer Fraud and Conspiracy to Commit Computer Fraud), 1344 (Bank Fraud), and 1349 (Conspiracy to Commit Bank Fraud) (hereinafter, collectively the “TARGET OFFENSES”).

3. In summary, beginning on or about July 27, 2024, through and including on or about August 6, 2024, BROWN conspired with another person(s) to defraud a victim bank located in the Western District of New York (hereinafter the “BANK”) by gaining unauthorized access to 12 customers’ online accounts and using that access to transfer funds out of the customers’ bank accounts without their knowledge or permission.

4. BROWN was an employee of the BANK. BROWN used his employee access to look up sensitive customer information, including bank account and social security numbers, and then provided that information to his co-conspirator(s). The co-conspirator(s), in turn, used this customer information to gain unauthorized access to the victim customers’ online accounts and transfer money out of their bank accounts.

5. As a result of this conspiracy, BROWN and his co-conspirator(s) stole approximately \$327,000 from the BANK and its customers.

6. This affidavit is intended to show that there is probable cause for the requested criminal complaint and does not set forth all my knowledge about this matter.

7. The facts contained in this affidavit are based upon my personal involvement in this investigation and information provided to me by other law enforcement agents and private companies.

PROBABLE CAUSE

A. Background regarding the BANK's online accounts

8. The BANK provides each of its customers with an online account. Through that online account, customers can review their bank account information and transfer funds.

9. In order to access an online account, a customer first needs to register that account.

10. A customer can do that by going to the BANK's website and providing his or her bank member number and social security number, as a means of authenticating the customer's identity.

11. When registering an online account, a customer also needs to provide an email address. The BANK automatically sends an authentication email that contains a verification code to the provided email address. The customer then enters the verification code to complete the online account registration.

12. Finally, a customer is required to accept the BANK's Terms & Conditions Agreement, which states: "You represent and warrant that you are who you claim to be; that you are the rightful owner of all Content and the Accounts linked for the purposes of the

Online Money Movement Service; and that you are rightfully authorizing us to access the Accounts.”

B. BROWN uses his employee access to look up customer information and provide it to his co-conspirator(s)

13. In or around August 2024, the BANK reported to the FBI that, between on or about July 27, 2024, and on or about August 6, 2024, someone accessed the online accounts of approximately 12 BANK customers and transferred funds out of those accounts, without the customers’ knowledge or consent.

14. Following the incidents, the BANK conducted an internal review of the victims’ accounts to determine how the accounts could have been compromised. As a result of this review, the BANK was able to determine that a specific BANK employee, BROWN, used his employee credentials to lookup each of the victim customers’ accounts around the time that those accounts were unlawfully accessed.

15. At the time that BROWN looked up the victim customers’ accounts, none of the victim customers were at a BANK branch or seeking assistance from BROWN.

16. Through these lookups, BROWN was able to see whether the victim customers had ever registered their online accounts. BROWN was also able to see the victim customers’ BANK member number and social security number.

17. Shortly after BROWN performed a lookup (typically on the same day), a co-conspirator(s) registered the victim customer’s online account.

18. BANK records showed that, the co-conspirator(s) used the victim customers' BANK member number and social security number when registering the victim customers' online accounts.

19. The co-conspirator(s) also accepted the BANK's Terms & Conditions and, in this way, falsely represented to the BANK that the co-conspirator(s) was each victim and was the rightful owner of each victims' online account.

20. Also while creating these online accounts, the co-conspirator(s) provided Google email accounts (hereinafter the "Google Target Accounts") and one Apple email account (hereinafter the "Apple Target Account" and together with the "Google Target Accounts" the "Target Accounts") for verification.

21. Once the co-conspirator(s) provided a Target Account, the BANK's system automatically sent a verification code to that Target Account. The co-conspirator(s) then obtained the access code from the Target Account and completed the registration process.

22. The victim customers were unaware that their online accounts had been accessed and had not given anyone permission to do so.

23. Once the online accounts were accessed, without the victim customers' knowledge or consent, BROWN and/or his co-conspirator(s) transferred money from the victim customers' accounts to third party accounts, also without the victim customers' knowledge or consent.

24. In total, BROWN and/or his co-conspirator(s) transferred approximately \$477,000 from 12 victim customers' accounts without their knowledge or consent.

25. BROWN and/or his co-conspirator(s) transferred the victim customers' money to other, third-party accounts held at the BANK.

26. Ultimately, approximately \$327,000 of the victim customers' funds were withdrawn as cash from various local branches. Some additional funds were also transferred through CashApp.

27. The third parties who received the unauthorized transfers and withdrew the cash had no apparent relationship to the victim customers.

28. Within a few days of these fraudulent transfers, a number of the victims contacted the BANK to report the unauthorized activity on their accounts. Following these notifications, the BANK confirmed with all of the victims that they had not accessed their online accounts, had not allowed anyone else to access their online accounts on their behalf, and had not requested or authorized any of the transfers.

C. Victim Customer 9

29. As an example of how this conspiracy worked, the following paragraphs detail when and how Victim Customer 9's online account was registered, accessed, and used to steal funds from Victim Customer 9.

30. According to the BANK's records, on or about July 31, 2024, at approximately 1:45 PM, BROWN looked up the account information for Victim Customer 9.

31. The next day, on or about August 1, 2024, BROWN or his co-conspirator(s) used Victim Customer 9's bank member number and social security number to register Victim Customer 9's online account.

32. According to records obtained from the BANK and AT&T, BROWN's cell phone number is XXX-XXX-0530.

33. Toll records from AT&T showed that, on or about August 6, 2024, BROWN called phone number XXX-XXX-9021 three times. The first two calls were 0 seconds in duration, the third call was 2 seconds.

34. BROWN called using an Apple iPhone 14 Pro bearing IMEI 35715467992507.

35. According to open-source research and NYSP records, the phone number XXX-XXX-9021 has been assigned to an individual who will hereinafter be referred to as Subject A since at least July 26, 2024.

36. While registering Victim Customer 9's online account, BROWN or his co-conspirator(s) provided the email address jonbaggie@icloud.com (*i.e.*, the Apple Target Account).

37. The same day that BROWN called phone number XXX-XXX-9021 three times, on or about August 6, 2024, BROWN and/or his co-conspirator(s) accessed Victim 9's online account and used it to transfer approximately \$30,436.70 out of Victim Customer 9's BANK accounts.

38. A member of the BANK's fraud team interviewed Victim Customer 9 and he/she confirmed that he/she never registered the online account, never gave anyone permission to register the online account, and never gave anyone permission to transfer \$30,436.70 out of that account.

D. Search of the Apple Target Account

39. On or about February 24, 2025, the FBI obtained a warrant, signed by the Hon. Mark W. Pedersen, to search the Apple Target Account. Upon executing that warrant, law enforcement found the following:

40. The Apple Target Account was created on May 27, 2024, using phone number XXX-XXX-3011, which was maintained by the phone provider TextMe. According to records obtained from TextMe, XXX-XXX-3011 was registered using IP Address 104.229.205.25 (hereinafter "IP Address 1").

41. According to records obtained from Charter Communications, IP Address 1 was assigned to Subject A from January 2, 2020, through July 14, 2024.

42. IP Address 1 was used to access the Apple Target Account three times on May 28, 2024, the day after the account was created.

43. IP Address 2603:7081:1d00:5b87:8c7a:1565:5fa8:7b39 (hereinafter "IP Address 2") was used to access the Apple Target Account once on May 31, 2024, four times on June 1, 2024, once on June 3, 2024, and once on June 25, 2024. According to records obtained from Charter Communications, IP Address 2 was assigned to Subject A from December 17, 2020, to July 18, 2024.

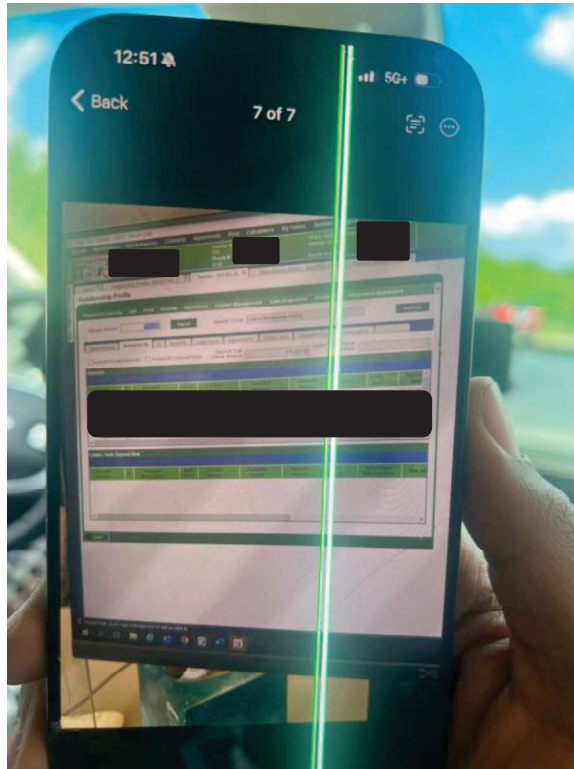
44. IP address 2603:7081:1d00:5b87:6caa:ca9d:4756:791c (hereinafter “IP Address 3”) was also used to access the Apple Target Account on June 25, 2024. According to records obtained from Charter Communications, IP address 3 was assigned to Subject A from January 2, 2020, through July 14, 2024.

45. T-Mobile IP Address 172.59.176.152 (hereinafter “IP Address 4”) was used to access the Apple Target Account on July 25, 2024. Less than 24 hours later, IP Address 4 was used to access Victim Customer 1’s online account.

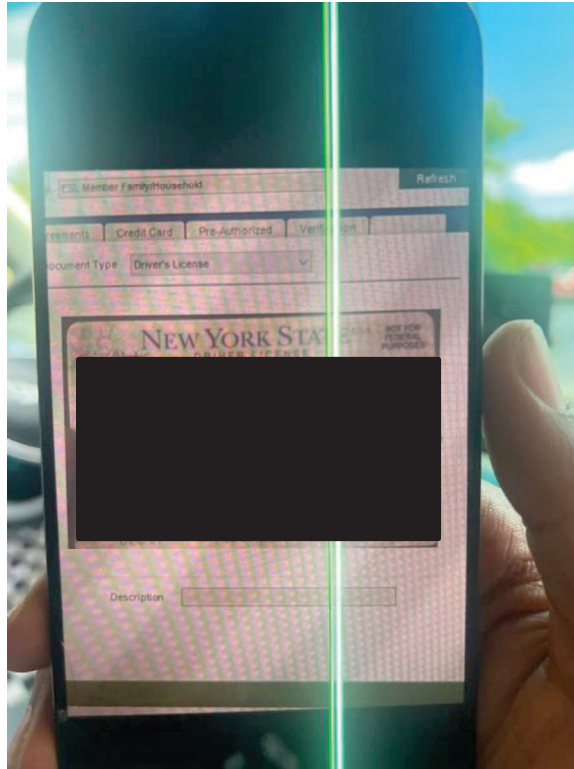
46. On or about July 25, 2024, and every day between July 27, 2024, and August 8, 2024, 14 other IP addresses were used to access the Apple Target Account. All of these IP addresses were T-Mobile IP addresses. According to records obtained from T-Mobile, the company had not maintained any subscriber records for these additional IP Addresses. According to T-Mobile, the company does not keep records on certain IP Addresses as part of its policy.

47. A number of IP addresses connected to the Apple Target Account between May 31, 2024, and August 8, 2024—including IP Address 2, which was assigned to Subject A, and the 14 T-Mobile IP addresses described above—were associated with automatic updates carried out by Apple for Applications including Facebook, Instagram, and TextMe. Based upon the connection logs provided by Apple, all of these connections were made by the same device (global_unique_id 00008110-00027CD41E38801E) and associated with the same iCloud account (person_id 21753411356). Based on my training and experience, I know that this indicates that the same device was used to access the Apple Target Account between May 31, 2024, and August 8, 2024.

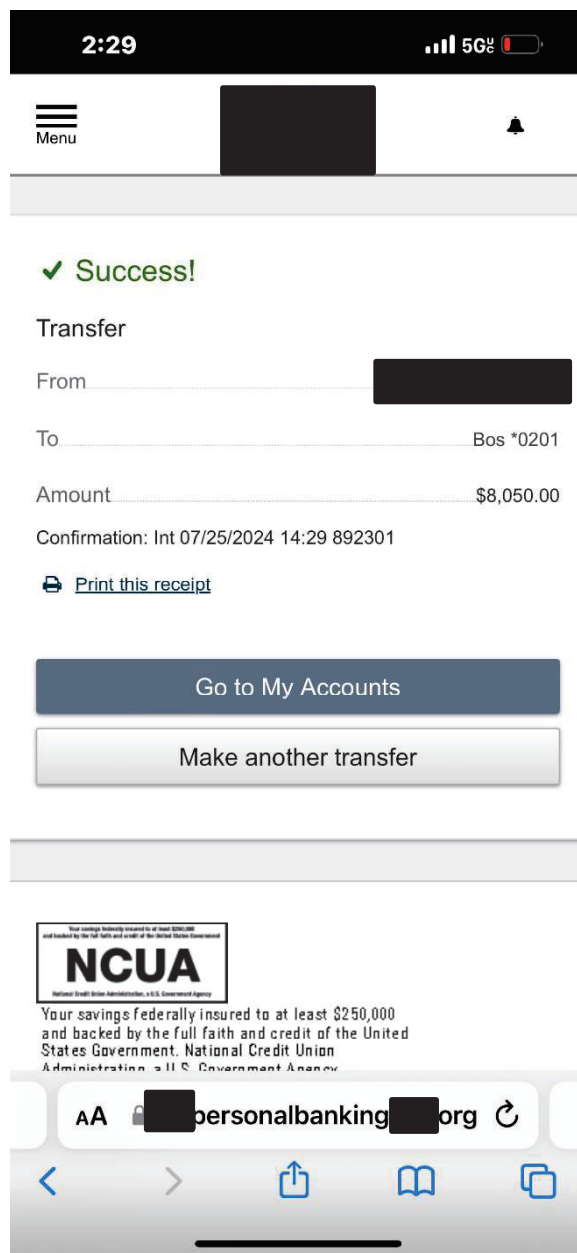
48. The Apple Target Account's photo library included the following images:
- a. A picture of an iPhone with a picture of a computer screen, which showed a BANK employee access page, where an employee could query BANK customer information. On the page were lookups for different BANK customers, including Victim Customer 1, as shown (with redactions) below:



- b. Five pictures of what appears to be the same iPhone with pictures of victim customers' driver's licenses taken from the BANK's internal database, as shown (with redactions) below:



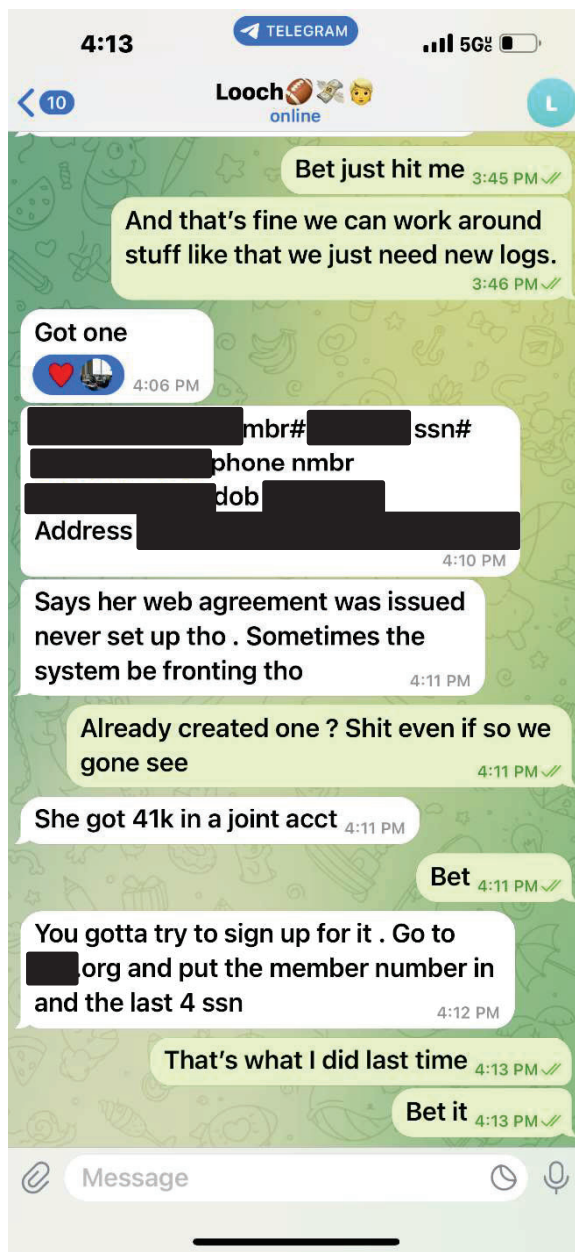
- c. Screenshots showing the successful online transfer of funds out of Victim Customer 1's BANK account, as shown (with redactions) below:



- d. Screenshots showing online account access to and the successful online transfer of funds out of Victim Customer 2's BANK account.

- e. Screenshots showing the online account registration for Victim Customer 3 as well as the successful online transfer of funds out of Victim Customer 3's BANK account.
- f. Screenshots of the online transfer of funds out of Victim Customer 4's BANK account.
- g. A screenshot of the successful online transfer of funds out of Victim Customer 6's BANK account.
- h. A screenshot showing the online account registration for Victim Customer 7.
- i. A screenshot showing the online account registration for Victim Customer 8.
- j. A screenshot showing the CashApp account that was used to receive stolen funds from Victim Customer 8's bank account.
- k. A screenshot showing the online account registration for Victim Customer 10.

1. A screenshot of a conversation on Telegram with Telegram user "Looch," in which "Looch" provided the name, bank account number, social security number, phone number, DOB, and address of Victim Customer 10, as shown (with redactions) below:



The FBI was not able to obtain subscriber information associated with the Telegram user “Looch.” However, the FBI was able to determine, through open-source research, that BROWN’s phone is associated with Snapchat account “looch_05” and TikTok account “DBL00CH.” The accounts also contained profile pictures of BROWN. Based on the similarity of the usernames, BROWN’s known involvement in the execution of this scheme, as set forth herein, and my training and experience in the investigation of cybercrimes, I respectfully submit that there is probable cause to believe that BROWN owns and controls the Telegram account “Looch” and was the author of the correspondence pictured above.

m. A screenshot of a conversation on Telegram with Telegram user “Beeju” in which “Beeju” provided the names and bank account numbers of unidentified victims who appeared to be customers at the same BANK, as shown (with redactions) below:



49. The FBI showed the images described in Paragraph 48 to the BANK, and the BANK confirmed that some of the pictures were of the BANK's internal records and corresponded with BROWN's activity, described above. Specifically, the pictures showed the date, time, location, and terminal station used to look up the information displayed in the photo. These matched the BANK's records regarding BROWN's activity on the network. Moreover, the BANK confirmed that the customers seen in the pictures being queried, including Victim Customer 1, had only been queried by BROWN at that time.

50. Based on this evidence and my training and experience in similar investigations, I respectfully submit that these images establish probable cause to believe that BROWN used his iPhone 14 or a similar device to take pictures of the customer information that he looked up and then send that information to his co-conspirator(s).

E. Search of the Google Target Accounts

51. On or about January 11, 2025, the FBI obtained a warrant, signed by the Hon. Mark W. Pedersen, to search the Google Target Accounts for evidence of the TARGET OFFENSES.

52. Upon executing that warrant, law enforcement found verification emails sent from the BANK containing one-time password (OTP) codes and notification emails sent from the BANK with updates regarding the victim customers' online accounts, including email updates, password resets, and account freezes.

53. Google's records also indicated that each of the Google Target Accounts had at least one IP Address that was used to access another Google Target Account. Similarly,

all but one of the Google Target Accounts linked to at least one other Google Target Account through website cookies. Based upon my training and experience, I know that website cookies are small files that are placed by websites onto a user's device during a browsing session. The Google Target Accounts were accessed from the same device and browsing session, indicating that the same individual accessed the accounts.

54. The Apple Target Account was accessed using the same IP Addresses that also accessed six of the Google Target Accounts, indicating that the same individual accessed both the Google Target Accounts and the Apple Target Account.

CONCLUSION

55. Based on the foregoing, I respectfully submit that there is probable cause to believe that BROWN committed the TARGET OFFENSES.

Respectfully Submitted,



JORDAN F. SLAVIK
Special Agent
Federal Bureau of Investigation

Affidavit submitted electronically by email in .pdf format. Oath administered and contents and signature attested to me and before me as true and accurate telephonically pursuant to Fed. R. Crim. P. 4.1 and 4(d) on June 24, 2025.



HON. COLLEEN D. HOLLAND
United States Magistrate Judge