



police officers were driving approximately one car length behind **BAH** and observed him on his cell phone while driving. The officers also observed **BAH** swerving out of the traffic lane, crossing over the double yellow line and onto the oncoming traffic on the other side of the road.

██████ initiated his police lights and pulled **BAH** over in front of 2441 Boston Road in the Bronx. He approached **BAH**'s vehicle on the front driver side and asked **BAH** for his license and registration. **BAH** handed a driver license bearing the name "Bah Thierno." ██████ observed him to be acting very nervously in that he was turning his body away from him, touching and hiding his wallet, as well as touching and shielding the front center cupholder console area of the car with his hands and body. ██████ asked **BAH** if there was anything in his vehicle. **BAH** did not respond; rather, **BAH** reached into his right pants pocket and took out another driver license bearing the name "Jared Buckley." ██████ asked **BAH** "What is that?" to which he did not respond.

██████ asked **BAH** to step out of the vehicle. Once **BAH** was out of the car, the police officers asked him "is that a fake ID?" **BAH** stated, in sum and substance, that he had grabbed the South Carolina driver's license with the name Jared Buckley from the center console and put it in his pocket. He admitted that the South Carolina license was fake, and he stated that he used it to get into clubs when he was younger. **BAH** then stated that he was 26 years old, but his birthdate was ██████. **BAH** then claimed he was 27 years old. He stated that he worked for Yellow Cab and had his taxi license. **BAH** stated that the Mercedes Benz was his brother's car, and that he had been driving it since the prior night.

██████ observed several credit cards and a card skimmer device in the front center cupholder console area of **BAH**'s car. ██████ also observed that the numbers affixed on the credit cards appeared blurry. Officers recovered a total of 29 credit cards, 3 drivers licenses,

AUSA       
 Defendant       
 Defense Counsel

and one skimmer device. **BAH** was placed under arrest at approximately 2:22 PM in front of 2441 Boston Road, Bronx, New York.

Detective [REDACTED] of the Bronx Grand Larceny Squad met with [REDACTED] at approximately 6:00 PM at the 49 PCT. Detective [REDACTED] ran the 29 credit cards through an electronic skimming device BIN (bank identification number) reader in order to determine whether the numbers of the magnetic strip on the credit cards matched the numbers on the front of the credit cards. Detective [REDACTED] ran all 29 of the credit cards through the BIN reader and the results of the BIN reader revealed that all 29 credit cards returned different information than what was represented on the cards themselves. In other words, all of the magnetic strips on the 29 credit cards were re-encoded and are forged.

Detective [REDACTED] also examined the skimmer device that had been recovered from the vehicle that **BAH** was driving. Detective [REDACTED] determined that this specific skimmer device is a Bluetooth device that can read information on the magnetic strip of a credit card, extract that information, and send that information to a neighboring computer or zip drive to be stored.

On August 22, 2019, a Bronx grand jury charged **BAH** with 30 counts of P.L. 170.25 Criminal Possession of a Forged Instrument in the Second Degree, 30 counts of P.L. 170.20 Criminal Possession of a Forged Instrument in the Third Degree, one count of P.L. 170.40(2) Criminal Possession of Forgery Devices, and one count of P.L. 190.85 Unlawful Possession of a Skimmer Device in the Second Degree.

After **BAH**'s arrest on July 31, 2019, he was released on his own recognizance pending trial. His case is still pending for trial before the Supreme Court of New York, Bronx County.



**Arrest on February 19, 2020, in Metairie, Louisiana**

On February 19, 2020, BAH and Manuela Gonzalez-Bookman, residents of the State of New York, were arrested for attempting to cash counterfeit checks on the accounts of victims using counterfeit identification, to include U.S. passport cards. On that date, Gonzalez-Bookman entered a Capital One Bank branch located at 1501 Veterans Blvd., Metairie, Louisiana. Capital One Bank, N.A., is an insured bank of the Federal Deposit Insurance Corporation. Gonzalez-Bookman attempted to cash a \$4,900.00 check against an existing Capital One account using a counterfeit U.S. passport card and a counterfeit credit card as identification. The name on the counterfeit passport card and counterfeit credit card were both the name of an actual Capital One account holder and New York resident, Victim A. However, the photograph on the passport card was Gonzalez-Bookman's. The check was from the Citibank account of Victim B, also a New York resident, with a memo line stating that it was for "Furniture Purchase."

Based on these circumstances, Capitol One employees became suspicious and contacted Jefferson Parish Sheriff's Office (JPSO) deputies. JPSO deputies arrived and detained Gonzalez-Bookman and gave *Miranda* warnings to her. Gonzalez-Bookman stated she understood those rights and agreed to speak with investigators. She admitted that she had flown in from New York and was attempting to cash a check fraudulently.

The Capital One branch manager advised deputies of what occurred earlier that day. An employee earlier that morning had seen a suspicious male walk into the bank, ask for a pen, and then return outside to a black SUV parked in the parking lot. Employees noted that the SUV was still parked there when Gonzalez-Bookman was in the branch. Employees went outside and noted the license plate [REDACTED] at which time the driver of the SUV backed his car up, in an apparent attempt to conceal his license plate. Around this time, bank employees contacted Victim

AUSA MP  
 Defendant TB  
 Defense Counsel KE

A and learned that he/she was not inside the branch, and he/she did not authorize anyone to cash a check against his/her account. Employees then called JPSO deputies to arrest Gonzalez-Bookman. When deputies arrived, the driver of the black SUV pulled out of the parking lot and drove away.

Deputies initially pulled over the suspicious black SUV. **BAH** identified himself to deputies. During the investigatory stop, the officers who were interviewing Gonzalez-Bookman were told by her that she had arrived in a small gray car. Deputies therefore released **BAH** due to Gonzalez-Bookman's statements.

As the interview with Gonzalez-Bookman progressed, however, she admitted that she actually had been driven to the bank branch in a black SUV. Deputies issued an alert for the black SUV. Deputies successfully located the black SUV and **BAH** later that day.

Deputies detained **BAH** and obtained a search warrant for the black SUV. The vehicle was towed to 1801 Westbank Expressway, Harvey, LA. During a search of the vehicle, deputies found various items, among which were an airline ticket in the names of **BAH** and Gonzalez-Bookman, as well as New York identification cards for Gonzalez-Bookman. Two of the airline tickets showed that **BAH** and Gonzalez-Bookman took the same United Airlines flight together from Newark Liberty International Airport to New Orleans International Airport (MSY) on January 30, 2020.

Deputies also found an envelope concealed in the headliner of the vehicle. The envelope contained four counterfeit credit cards along with four fraudulent identity documents with matching names to the credit cards. These fraudulent identity documents included: a U.S. passport card, an Alabama driver's license, a New Jersey driver's license, and an Oregon driver's license. All four fraudulent documents were bearing the photograph of Gonzalez-Bookman, but they were not in her name. The fraudulent U.S. passport card was in the name a person residing in Louisiana (Victim C). Deputies also found Citibank checks and Chase Bank checks concealed in the

headliner of the car. Agents obtained Hertz rental records that showed that **BAH** rented the vehicle at the MSY rental facility in the early morning of February 19, 2020.

The victims of these offenses confirmed that they did not give **BAH** or Gonzalez-Bookman permission to use their respective identities.

**Prior Fraud in Louisiana from January 30 to February 2, 2020**

Agents obtained flight records that showed that **BAH** and Gonzalez-Bookman previously traveled together to New Orleans between January 30 and February 2, 2020. Agents also contacted Capital One bank investigators, who provided information that showed a similar pattern of fraudulent activity that coincided with **BAH** and Gonzalez-Bookman's prior trip to New Orleans. In each of these instances, Gonzalez-Bookman is on surveillance video attempting to perform the transactions, similar to the transaction on February 19, 2020. Using Capital One records as well as airline records, agents were able to reconstruct the following timeline:

- On January 30, 2020, **BAH** and Gonzalez-Bookman took the same Southwest Airlines flight from LaGuardia International Airport to MSY.
- On January 31, 2020, at approximately 10:17 a.m., Gonzalez-Bookman successfully used the Capital One account of Victim D, a resident of New York, to cash a \$4,900.00 check written from the Wells Fargo account of Victim E, a resident of New Jersey. This transaction occurred at a Capital One branch in New Orleans.
- On January 31, 2020, at approximately 11:07 a.m., Gonzalez-Bookman successfully used the Capital One account of Victim D to cash a \$4,760.00 check written from Victim E's Wells Fargo account. This transaction occurred at a Capital One branch in Metairie, LA.



- On January 31, 2020, at approximately 12:34 a.m., Gonzalez-Bookman attempted to withdraw \$18,600.00 in cash from Victim D's account, but the transaction was declined. The attempted transaction occurred at a Capital One branch in Destrehan, LA.
- On February 1, 2020, at approximately 9:32 a.m., Gonzalez-Bookman successfully used the Capital One account of Victim F, a resident of Louisiana, to cash a \$4,800.00 check written from Victim E's Wells Fargo account. This transaction occurred at a Capital One branch in Baton Rouge, LA.
- On February 1, 2020, at approximately 10:21 a.m., Gonzalez-Bookman successfully used the Capital One account of Victim F, to cash a \$4,900.00 check written from Victim E's Wells Fargo account. This transaction occurred at a second Capital One branch in Baton Rouge, LA.
- On February 1, 2020, at approximately 11:25 a.m., Gonzalez-Bookman successfully used the Capital One account of Victim F, to cash a \$4,880.00 check written from Victim E's Wells Fargo account. This transaction occurred at a third Capital One branch in Baton Rouge, LA.
- On February 2, 2020, **BAH** and Gonzalez-Bookman took the same Spirit Airlines flight from MSY to Newark Liberty International Airport.

**Search of BAH's Cell Phone**

JPSO deputies obtained a search warrant for **BAH's** cell phone that was recovered from him during his arrest on February 19, 2020. Agents reviewed the contents of **BAH's** cell phone and found additional evidence of fraud.

**BAH's** phone had text messages, WhatsApp messages, and other information that confirmed that the phone was **BAH's**. For instance, agents found photo of a computer screen showing a for-hire driver license application for "Thierno Bah", and with email address [REDACTED] WhatsApp messages showed that **BAH** communicated with the name "Wayne Bah," which confirms that **BAH** used the moniker "Wayne Bah" as well.

**BAH's** phone contained evidence of a conspiracy to commit fraud. Agents found photographs of false identification cards, such as false New Jersey and Michigan drivers licenses with photos of unknown individuals. Agents also found a photo of a false United States passport card with **BAH's** photo but with another name imprinted on it.

Agents also found photographs that corroborated **BAH's** participation in the fraud in Louisiana. Agents recovered a photograph of a handwritten note that contained Victim F's personal information, including her name, address, social security number, date of birth, her current account balance, and her last transaction amount at Capital One Bank. Capital One confirmed that the information for Victim F's account on **BAH's** phone was accurate as of the date of the fraud.

Agents also found evidence of communications with co-conspirators who appeared to be engaging in fraud. For example, agents found a photograph of text messages between two individuals in which one of them stated "[I]m in the bank I cant be texting," to which the other person replied with four texts: "[s]end yah [expletive] location," and then "I told you don't go in there without be Bozo," followed by "If u have the debit card on u," and finally, "Wait for me don't leave we coming."

Agents also found evidence of numerous stolen identities and accounts. Agents found



screenshots from cell phones and computers that were from websites on the dark web that sell stolen account information. One photograph had information for five different stolen bank accounts, and they included the cardholder's name, address, date of birth, and other identifying information.

**Additional Fraud Corroborated from BAH's Cell Phone**

Agents continued their investigation to determine whether **BAH** or any of his co-conspirators had used these stolen identities and accounts to commit fraud. By search **BAH's** cell phone and then contacting financial institutions, agents were able to piece together a history of fraud by **BAH** and his co-conspirators. They show that **BAH** has committed fraud using stolen credit card information since at least 2018. More recently, **BAH** has also committed fraud by using false or stolen checks, which is consistent with the fraud committed in Louisiana in January and February 2020. The following is a summary of the fraudulent conduct that agents were able to corroborate.

- On July 6, 2018, **BAH** sent a WhatsApp message to an individual called "Pop". That message included the following information of Victim G, a resident of Texas: name, city and state of residence, credit card number, expiration date, CVV code, and telephone number. On the same day, July 6, 2018, a fraudulent charge for an AT&T bill payment of \$433.54 was made on this credit card account. At the time of the fraudulent charge, the credit limit on Victim G's account was \$34,000.00.
- On February 18, 2019, **BAH** sent a WhatsApp message to an individual named "Pelle." That message included the following information of Victim H, a resident of New York State: credit card number, expiration date, and CVV code. On the same day, February 18,

2019, this credit card was used for a fraudulent charge at the Seton Hotel in New York of \$1,185.71. At the time of this fraudulent charge, the Victim G's credit limit was \$41,000.00.

- On February 18, 2019, **BAH** sent a WhatsApp message again to "Pelle." In this message, **BAH** sent the following information for Victim I, a resident of New York State: credit card number, expiration date, and CVV code. On February 24, 2019, the stolen credit card number was fraudulently used at a Holiday Inn in New York City, for \$924.67. At the time of the fraud, Victim I's credit limit was \$43,800.00.
- On June 10, 2019, the credit card number of Victim J, a resident of Vermont, was used to make a fraudulent charge to Lyft.com of \$23.85. Victim J's credit limit was \$8,000.00. On June 11, 2019, **BAH** sent Victim J's credit card number, expiration date, CVV code, and billing address by WhatsApp message to an unnamed person with a phone number ending in [REDACTED]
- From August 1 through August 3, 2019, the credit card number of Victim K was used to make a total of \$217.53 in fraudulent charges. The charges included taxi charges in Long Island City, New York. Victim K, a resident of Vermont, had a credit limit of \$13,000.00. On August 9, 2019, **BAH** sent Victim K's name, credit card number, expiration date, CVV code, and billing address via WhatsApp to a person identified as "Yaya Ab Man."
- On September 26, 2019, **BAH** received Victim L's credit card information via WhatsApp from the unnamed person with phone number ending in [REDACTED]. Victim L is a resident of Iowa. **BAH** received Victim L's name, occupation, billing address, credit card number, expiration date, and CVV code. On October 30, 2019 fraud subscriptions were started

against Victim L's credit card account. These included charges for a VPN masking service (\$14.95) and a virtual business phone system called Grasshopper.com (\$37.39). Based on agents' training and experience, a VPN masking service and virtual phone system can be used in furtherance of a fraud conspiracy. The total charged was \$157.02. Victim L's credit limit at the time of the fraud was \$2,000.

- On October 13, 2019, **BAH** sent a WhatsApp message to a person identified as "40-100." **BAH** sent the following information for Victim M, a resident of Florida: billing address, credit card number, expiration date, and CVV code. At this time, **BAH** and "40-100" also discussed movie tickets. On the same date, October 13, 2019, there is a fraudulent charge for \$47.38 on Victim M's credit card at a movie theater. Victim M's credit limit at the time of the fraud was \$4,800.00.
- Between December 11, 2019, and December 20, 2019, three fraudulent checks were written against the checking account of Victim N, a resident of Connecticut. These three checks totaled \$18,741.31. Victim N's bank, however, discovered the fraud and stopped the checks from clearing. During a search of **BAH**'s phone, agents found two photographs of fraudulent checks from Victim N's checking account. The metadata on these photographs show that they were made on December 17, 2019. The photo is of check [REDACTED] which is the check that the perpetrators attempted to deposit on December 20, 2019.
- On January 21, 2020, three fraudulent checks totaling \$600.00 were cashed on the checking account of Victim O, a company based in Chicago Heights, Illinois. During a search of **BAH**'s phone, agents found that **BAH** had a photo of a check from Victim O's



account. The metadata on the phone showed that the photograph was taken on January 23, 2020.

- On January 24, 2020, **BAH** sent a WhatsApp message to a person identified as “TT 116th”. **BAH** sent the following information for Victim P, a resident of Kentucky: name, date of birth, address, height, and eye color. Victim P had four bank accounts at Chase Bank. On February 13, 2020, **BAH**’s conspirators opened four fraudulent Chase Bank accounts. These four accounts were joint accounts in the name of Victim P and a false identity. Victim P did not open these accounts, however. Moreover, the conspirators also changed the billing on two of Victim P’s legitimate accounts from Kentucky to an address in Bronx, New York. Agents found a photograph on **BAH**’s phone of an attempt to create a Gmail account that used Victim P’s name in the email address. On February 14, 2020, a total of \$92,625.00 was then transferred out of Victim P’s four legitimate accounts and into the four fraudulent joint accounts naming Victim P and fictitious individuals. The conspirators then transferred the funds into other accounts in an attempt to complete the theft. Chase Bank, however, was able to freeze most of the funds, and the lost funds totaled \$4,784.43.


Sentencing Stipulation

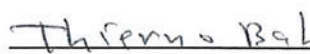
For the purposes of sentencing only, the parties agree that the total intended loss amount caused by **BAH**’s conduct and the reasonably foreseeable conduct of his co-conspirators was between \$250,000.00 and \$500,000.00.


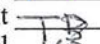
Limited Nature of Factual Basis

This proffer of evidence is not intended to constitute a complete statement of all facts known by **BAH**, and it is not a complete statement of all facts described by **BAH** to the government. Rather, it is a minimum statement of facts intended to prove the necessary factual predicate for his guilty plea. The limited purpose of this proffer is to demonstrate that there exists a sufficient legal basis for **BAH**'s plea of guilty to the charged offense.

 7/13/2021  
\_\_\_\_\_  
Matthew R. Payne Date  
K. Paige O'Hale  
J. Ryan McLaren  
Assistant United States Attorneys

 6/10/2021  
\_\_\_\_\_  
Kareem El Nemr Date  
Counsel for Thierno O. Bah

 7/10/21  
\_\_\_\_\_  
Thierno O. Bah Date  
Defendant

AUSA   
Defendant   
Defense Counsel 