

UNITED STATES DISTRICT COURT
for the
Southern District of Florida

FILED BY KJZ D.C.

Jul 13, 2020

ANGELA E. NOBLE
CLERK U.S. DIST. CT.
S. D. OF FLA. - West Palm Beach

United States of America)
v.)
EDTRONDA SIMON,)
)
)
)
)
Defendant(s)

Case No. 20-8241-WM


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 see attached affidavit in the county of Palm Beach and elsewhere, in the
Southern District of Florida, the defendant(s) violated:

<i>Code Section</i>	<i>Offense Description</i>
Title 18, United States Code, Section 1029(a)(2)	Access Device Fraud
Title 18, United States Code, Section 1344	Bank Fraud
Title 18, United States Code, Section 1028A	Aggravated Identity Theft

This criminal complaint is based on these facts:
see attached affidavit.



Certified to be a true and correct copy of the document on file
Angela E. Noble, Clerk,
U.S. District Court
Southern District of Florida
By Kenneth J. Zuniga
Deputy Clerk
Date Jul 13, 2020

Continued on the attached sheet.

S. Schaut / PPD + USSS
Complainant's signature

Sarah Schaut, Task Force Officer, USSS
Printed name and title

Sworn and Attested to me by Applicant by Telephone (FaceTime)
per Fed.R.Crim.P. 4(d) and 4.1,

Date: **July 13, 2020**

William Matthewman
Judge's signature

City and state: West Palm Beach, FL

William Matthewman, U.S. Magistrate Judge
Printed name and title

AFFIDAVIT

I, **Sarah Schaut**, being first duly sworn, hereby depose and state as follows:

1. I am employed with the Plantation Police Department and currently assigned to the Criminal Investigations Division (CID) as an Economic Crimes Detective. I have been employed in a law enforcement capacity since April 2011, with the past three years assigned to CID. I have been sworn as a Task Force Officer (TFO) with the United States Secret Service (USSS) since January 2019 and assigned to the South Florida Organized Fraud Task Force of the Miami Field Office. I have been trained to conduct criminal investigations involving or relating to the financial infrastructure of the United States, including identity theft, counterfeit United States currency, wire fraud and access device fraud. I have completed the Basic Recruit Certificate of Compliance for Law Enforcement Officers at the Institute of Public Safety, Davie, FL.

2. The facts in this affidavit come from my personal observations, my training and experience, review of police reports, and information obtained from other law enforcement officers and witnesses. Because this affidavit is provided for the limited purpose of establishing probable cause for the charges in the Complaint, this affidavit does not set forth every fact known to me regarding this investigation.

PURPOSE OF THE AFFIDAVIT

3. This affidavit is submitted for the limited purpose of establishing probable cause that EDTRONDA SIMON committed the offenses below:

- In or around 2016, and continuing through the present, the exact dates being unknown, in Palm Beach County, Florida, and elsewhere, Edtronda SIMON did knowingly and with intent to defraud use one or more unauthorized access devices during a one year period, and by such conduct, obtain anything of value aggregating \$1,000 or more during that period, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Sections 1029(a)(2) and 2; did knowingly execute a scheme or artifice to obtain any of the moneys, funds, and credits, owned by, or under the custody or control of, a financial institution by means of false or fraudulent pretenses, representations, or promises, in violation of Title 18, United States Code, Sections 1344 and 2; and during and in relation to an enumerated felony

.did knowingly use, without lawful authority, a means of identification of another person, in violation of Title 18, United States Code, Sections 1028A and 2.

THE GENERAL SCHEME

4. Your affiant is a member of a task force investigating an ongoing bank fraud scheme targeting elder victims living in South Florida. Based upon victim interviews and contact with the affected financial institutions, this section provides a general overview of how the fraud scheme generally works.

5. In general, each individual victim is telephonically contacted by a professional sounding caller. To your affiant's knowledge, the caller is always a female. That caller states that she is a bank representative from the victim's bank. The caller tells the victim, falsely, that the victim's account has been compromised.

6. The bank and account type vary with each victim, but in general the caller is attempting to get access to the victim's credit and debit cards. According to the victims, the caller supplies banking information regarding the victim's account that convinces each victim that the call is legitimate. For example, multiple victims have stated that the caller had their last transaction information. The caller will then include some fictitious transaction descriptions with the legitimate transaction descriptions, which then convinces the individual victim that their account or bank card has been compromised.

7. The caller then offers to send a "bank representative" to the victim's home to exchange the "compromised" card with a new one. The victims report a "bank representative" arrives at their residence shortly thereafter, usually while the victim is still on the phone with the original caller. The "bank representative" then obtains the victims "compromised" debit and/or credit card(s) with the promise of returning with a new uncompromised card. Usually the caller has already convinced the individual victim to verify his or her PIN number. After the "bank representative" leaves with the compromised cards, that representative and another coconspirator then spend money as quickly as possible, often withdrawing cash from ATMs, purchasing money orders from Publix, and otherwise using the accounts as quickly as possible. Surveillance video obtained from the various stores and ATMs shows that the suspects utilizing the cards are often

speaking on the telephone with an unknown person while at the Publix/Store or bank ATM machine.

8. This fraud scheme has been ongoing since at least 2016 and continues through the present. Law enforcement and financial institutions have identified over 250 individual victims identified in Broward, Palm Beach, St. Lucie, and Indian River Counties, and elsewhere. Most of the victims are elderly and living in retirement communities. The financial institutions report more than \$1,000,000 in financial loss. While some arrests of persons responsible for using the cards have been made by local police departments, the group tends to move operations to different counties when one area becomes too hot. All victims described below resided in the Southern District of Florida.

9. The person calling the victims and the banks is believed to be SIMON, who used different phones to call the victims and the banking institutions. On occasion, SIMON was recorded by banks pretending to be various victims in an effort to have the bank raise spending limits, approve transactions, or provide other information in furtherance of the fraud scheme. SIMON switched phones frequently and uses prepaid phones and/or fictitious subscriber information to make detection and collection of evidence by law enforcement more difficult.

THE COOPERATING DEFENDANT

10. In spring 2019, a member of the group was charged by the Palm Beach County State Attorney's office on fraud charges related to his/her participation in the scheme. The cooperating defendant (CD) had been identified as one of the "bank representatives" entering victim's residences to retrieve their "compromised" bank cards from the elderly victims. The CD then purchased money orders, made ATM withdrawals, or purchased goods using the victim's cards and PIN numbers. Law enforcement had identified the CD in numerous cases from surveillance video and victim identifications.

11. After the CD was arrested, in a post-*Miranda* statement, the CD admitted participating in the scheme with others on 30 to 40 occasions in South Florida between December 2018 and March 2019. The CD identified the ring leader as SIMON, who the CD has known since they were teenagers, and when SIMON lived in South Florida. SIMON had moved to the Atlanta area from South Florida, but continued to participate in the scheme. According to the CD, SIMON picked the victims, called each victim, and was

the person who called the related financial institutions. While SIMON was on the phone with the victim and the bank, the CD and another co-conspirator (a driver) would go to the victim's residence. While the driver remained outside, the CD would go inside, meet with the victim, and collect the victim's bank cards, which the CD and the driver then used as quickly as possible per SIMON's instructions.

12. The CD consented to the search of his/her cellular telephone, which was in the CD's possession on the date of the CD's arrest. The CD identified SIMON's cellular telephone number as a phone with a 404 area code, ending in 4664 (Phone 4664). Stored text messages within the CD's phone were consistent with the CD's description of SIMON's role, as described in further detail below.

13. During the interview, the CD identified SIMON's voice from calls captured by Bank of America and Wells Fargo, in which SIMON impersonated a victim. SIMON asked specific questions related to victims' accounts, such as the ATM withdrawal limit amounts and maximum amounts authorized at a Point of Sale terminal.

CASES INVOLVING COMMUNICATIONS WITH PHONE 4664 AND SIMON

14. On March 9, 2019, victim "S.J." received a phone call from a female claiming to be "Ashley" from Bank of America (BofA). Ashley notified S.J. that her bank cards were compromised and fraudulent charges were made onto the cards. Ashley requested S.J. to verify her PIN number, which S.J. provided. During their hour-long phone conversation, the CD arrived at S.J.'s home, pretending to be a bank representative, and S.J. gave the CD her credit card and debit card.

15. BofA later notified S.J. that multiple fraudulent charges were made on her debit card and credit card; for a total of \$2,514.57. One of the fraudulent charges was made at a Publix at 1:51 pm for the purchase of \$1,502.67 in money orders. Surveillance footage showed that the person purchasing the money orders was the CD.

16. The CD's cell phone showed the following text messages with Phone 4664 (used by SIMON) on March 9, 2019, the day the co-conspirators targeted S.J. At 12:12 pm, Phone 4664 texted the CD that a victim was ready and waiting. At 1:40 pm, Phone 4664 messaged CD to go to Publix. At 1:48 pm, Phone 4664 messaged CD the correct PIN number for S.J.'s card, which S.J. had provided to the fraudulent BofA representative who had called. The timeframe of the text messages between SIMON and the CD

correlates with the timeframe of the phone calls received by S.J. and the video captured at Publix.

17. On February 24, 2019 at approximately 10:10 am, victim "D.R." received a phone call from "Ashley" claiming to be from BofA. Ashley informed D.R. that her bank cards were compromised and were fraudulently used. D.R. was told that a bank representative would respond to the residence to collect the cards. At approximately 12:00 pm, the CD arrived at the victim's home, and collected the bank cards along with their respective PINs. D.R. was instructed that someone would return to the residence with new cards.

18. While still on the phone with Ashley, D.R. received several legitimate text messages from BofA asking if recent charges were authorized. Ashley directed D.R. to respond "yes," indicating that D.R. did authorize the recent charges. At approximately 4:00 pm, Ashley claimed to have resolved all fraudulent charges and ended the call. When no representative returned with new cards, D.R. grew suspicious, contacted BofA, and discovered that approximately \$14,000 was charged to the cards from Publix, Best Buy, and by ATM withdrawals.

19. Surveillance footage from Publix and Best Buy showed that the CD was using D.R.'s cards at those locations. Also on February 24, 2019, Phone 4664 (used by SIMON) sent two photographs of D.R.'s BofA bank cards to the CD via text message, which D.R. sent to "Ashley" during their phone conversation. BofA also captured Phone 4664 calling its Customer Service line to increase the purchase and ATM limits on D.R.'s account.

20. BofA and Wells Fargo investigators verified that Phone 4664 called the banks in connection with at least 8 reported frauds where victims' cards were taken and subsequently used without authorization. These incidents occurred between the dates of February 19, 2019 and March 27, 2019.

OTHER RELEVANT CELL PHONES

21. On November 22, 2019, victim S.S. reported receiving a telephone call from a telephone number ending in 9459 (Phone 9459), from a person claiming to be from the Chase Bank Fraud Department. According to S.S., the caller stated that S.S.'s and R.S.'s accounts had been hacked, that money had been removed, and the police had a suspect in custody at Walmart. S.S. said the caller had all S.S.'s account information, including

PIN numbers. The call lasted three hours, during which time the caller told S.S. that a bank representative would come pick up their compromised cards.

22. While the caller was still on the line, a female “bank representative” arrived, to whom S.S. gave several Citibank cards. S.S. and R.S. became suspicious and contacted the police that evening. Citibank informed S.S. that \$8000 had been withdrawn from their various bank accounts using an ATM machine located in Broward County. S.S. was informed that an unknown person had transferred money between the accounts posing as the victim(s), and had also raised the account withdrawal limits.

23. Verizon Wireless¹ confirmed that Phone 9459 was assigned to a Tracfone that began making calls on November 21, 2019. Tracfone is a prepaid phone that does not require verification of the subscriber, and is provided service through companies such as Verizon. Call detail records confirmed Phone 9459 called S.S. on November 22, 2019. Call detail records also showed that Phone 9459 was used in a manner that was consistent with the fraud scheme. For example, between November 21, 2019 and December 17, 2019, Phone 9459 called multiple 800 numbers, that were associated with banks such as Wells Fargo, Chase Bank, and BofA. There are relatively few incoming telephone calls on Phone 9459, which is also consistent with the phone being used in the fraud scheme. There were also other lengthy calls that were consistent with calling other victims.

24. On November 30, 2019, a victim received a call from Phone 9459 from a female “bank representative” from Wells Fargo who convinced her there was fraud on her account. The victim met the bank representative in a parking lot to collect the victim’s PIN numbers and cards. The victim reported that approximately \$5800 was taken from the victim’s bank account through fraudulent withdrawals and the purchasing of money orders. Call detail records confirmed that Phone 9459 called the victim’s number on the date of the reported fraud, November 30, 2019.

25. Verizon confirmed that on December 17, 2019, Phone 9459 was changed to a number ending in 0844 (Phone 0844). SIMON then used Phone 0844 to further the fraud scheme, as described below.

¹ Throughout this affidavit, Verizon Wireless provided information pursuant to legal process.

26. On December 23, 2019, victim "N.R." received a telephone call from a female caller identifying herself as "Mary Jenkins," a representative of Citibank, who explained there was fraudulent activity on the victim's debit card. "Mary" told N.R. that there were 8 charges on N.R.'s card that were in question, and sent a representative from the bank to pick up the old card and bring a new one. A woman came to N.R.'s home, and picked up N.R.'s debit card, but did not bring a new card. Citibank later informed N.R. that \$3200.00 had been removed from the victim's Citibank account.

27. The victim showed the responding officer the victim's caller identification, which showed that Phone 0844 had called the victim. Verizon call detail records confirmed that Phone 0844 called the victim's number twice on December 23, 2019, with the calls lasting approximately 43 and 125 minutes each.

28. Phone 0844 was also identified by another victim, "D.W.," who claimed that s/he lost \$13,861.78 to fraudulent charges after providing a "bank representative" four (4) credit/debit cards on December 20, 2019. The victim reported that s/he was called by Phone 0844. Review of the Verizon call detail records for Phone 0844 confirmed that on December 20, 2019, Phone 0844 called D.W.'s telephone number multiple times.

29. Investigators learned of another number, Phone 9046 (also a Tracfone, with service provided by Verizon), which was linked to multiple incidents. For example, on December 31, 2019, victim "R.F." reported that she received a telephone call from a female caller claiming to be from BofA, and that R.F. had unauthorized transactions posted to her account. R.F. advised that the caller kept her on the phone for approximately three hours. The caller sent a BofA representative to R.F.'s home, who retrieved R.F.'s bank card.

30. BofA confirmed that fraudulent activity occurred on R.F.'s Bank of America checking account, and that on December 31, 2019, at approximately 5:18 pm, a person using Phone 9046 called BofA's Customer Service line to check the victim's balance and obtain information for the account's five most recent transactions. In addition, on December 31, 2019, at 5:39 pm, an unknown person called Bank of America customer service and increased the daily ATM withdrawal threshold. On the same date, R.F.'s Bank of America debit card was used for two fraudulent ATM withdrawals, for \$800.00 and \$1,400.00.

31. The same pattern occurred on January 2, 2020. Victim "M.C." gave her BofA cards to a fraudulent bank representative after a caller pretending to be from the bank told M.C. there was fraudulent activity on her account. BofA subsequently confirmed that on that same date, at 3:33 pm, a person using Phone 9046 called their customer service to check the victim's account balance and obtain information for the account's five most recent transactions. In addition, on January 2, 2020, at 3:54 pm a person used Phone 9046 called BofA customer service to transfer \$5,000.00 from M.C.'s saving account to her checking account. (To your affiant's knowledge, there were ultimately no withdrawal attempts on this account.)

SURVEILLANCE AT SIMON'S HOUSE and SUBSEQUENT SEARCH WARRANT

32. On January 16, 2020, agents observed two parked vehicles at **** Providence Point Way in Georgia, which they had identified as the location where SIMON lived (SIMON'S HOUSE). The cars were a Black Range Rover (tag obscured) and a lawn Trailer with Florida tag: #LSZU01. When the Florida license plate for the Trailer was later checked, the plate came back to Villashio Island Lawncare, LLC. SIMON's public Facebook page listed "Lady Villashio" as her nickname, and investigation had shown that SIMON is the registered agent and title manager to a hair care business called Villashio Exotic Hair LLC.

33. On February 5, 2020, victim "M.S." received three phone calls from Phone 8574. The female caller, representing herself as a Chase Bank representative, advised M.S. that there were fraudulent charges on her account. The caller requested M.S. to confirm her bank card number, which M.S. had difficulty doing without her glasses. M.S. told the female caller that she was not going to cancel her bank card and was uncooperative, resulting in the female caller disconnecting.

34. The USSS executed a court-authorized search warrant for SIMON'S HOUSE on February 5, 2020. Inside the house were SIMON and three men. The USSS seized a total of nineteen (19) electronics from the residence, along with six (6) hand written ledger notebooks that contained personal identification information (PII) of others. The ledgers were processed for latent prints to determine additional evidentiary value. A total of three latent prints were successfully retrieved from the ledgers. Two of the three did not produce any positive match due to insufficient ridge details; however, the third

print produced a positive match through the Automated Fingerprint Identification System (AFIS) to SIMON. A further review of the ledgers determined that a total of 573 individuals' names, birthdates, social security numbers, residential addresses, and bank account information were written down. When the ledgers were compared to documented police reports with the exact scheme described above, 35 of the individuals listed were confirmed victims.

35. During the execution of the search warrant, SIMON and the others were escorted out of the residence. While SIMON was walking out of the residence, she attempted to hide a cell phone under her arm, in her arm pit area. That phone was subsequently seized and is pending analysis. There were no arrests made during the search warrant, and SIMON remains at large. SIMON moved out of SIMON's HOUSE after the execution of the search warrant, and the USSS is unaware of her whereabouts.

36. The USSS executed an amended court-authorized search warrant for SIMON's HOUSE on February 7, 2020, and discovered Phone 8574, which was a flip phone that had been broken in half, inside of a garbage can., Verizon had notified law enforcement that Phone 9046, which had been used in the scheme, had been changed to Phone 8574 on January 15, 2020.

FORENSIC ANALYSIS OF THE SEIZED ELECTRONICS FROM SIMON's HOUSE

37. The USSS has been unable to analyze multiple telephones found in SIMON's HOUSE, as they are password protected and encrypted. However, the USSS has been able to analyze some of the telephones, as described below.'

38. Forensic analysis of one Apple iPhone 7 which was found in the master bedroom of the residence, showed that SIMON was the owner and user of the cell phone, and that she used the phone to facilitate the ongoing scheme. The phone number for the phone was 470-401-8095 (area code from Atlanta, Georgia). The listed owner of the phone was "Villashio's iPhone," with the Apple ID registered to e-mail address villashioexotichaironline@gmail.com, the name of SIMON's hair care company. The contents of the phone show that it was primarily used for business purposes relating to the sale, price negotiation, and shipment of hair products. Multiple SMS text message conversations are displayed between customers and the owner of the business, SIMON. On January 31, 2020 a text message thread between a customer and SIMON shows

SIMON stating "We located in Atlanta" when the customer inquired about the business's location.

39. On January 25, 2020 an e-mail was sent to the phone's registered Apple ID e-mail from JP Morgan Chase Bank. The contents of the e-mail are personally addressed to SIMON relating to the signing up of paperless communication. Multiple additional e-mails are also personally addressed to SIMON, such as another e-mail dated January 25, 2020 relating to a new Chase ATM/Debit card for the business ROYAL HAIR LLC, another business for which SIMON is the registered agent and title manager.

40. A record of searched items through internet applications were captured on the cell phone. Multiple South Florida zip codes and financial institutions were searched; as well as respective Publix locations and the customer service phone numbers of several banks. Specifically, on February 4, 2020 "33437 chase bank boynton" was searched multiple times. When compared to the documented police reports, victim "L.S." received a phone call from a female representing herself from Chase Bank. An individual responded to L.S.'s residence (located in zip code 33437) and collected her bank cards and PIN number. L.S. then had \$3,000 fraudulently withdrawn from her Chase account.

41. A review of other additional cell phones found in SIMON's HOUSE exhibited behavior consistent with the scheme. These phones were primarily flip phones, did not have any names or contacts saved to the relating phone numbers, and the majority of the calls on the phones were outgoing. Investigation into the phone numbers that were called determined that multiple different financial institution's customer service numbers were dialed, along with numerous elderly individuals, primarily in the South Florida area. It should be noted that on several calls made to elderly individuals the function of *67 was used before the phone number, signifying that the phone operator was attempting to conceal the phone number from the recipient.

42. Another phone found in the house during the search displayed the pattern as described above. On February 5, 2020, an outgoing call was made to victim M.S. documented above. On February 4, 2020 an outgoing call was made to an 847 area code phone number for a total of 27 minutes and 57 seconds. A comparison to documented police reports determined that the phone number dialed was registered to victim "L.S.", who was previously mentioned above relating to contents found on the Apple iPhone 7.

FINANCIAL EXAMINATION OF SIMON'S ACCOUNTS

43. Like the telephones, SIMON used multiple bank accounts for short periods of time in furtherance of the conspiracy. To date, the USSS has identified and analyzed three bank accounts belonging to SIMON. The USSS obtained records for one BB&T Bank account (Account #6198) in SIMON's name, for approximately September 2016 through June 2017, which to the knowledge of your affiant was when the scheme was known to have started. Over the analysis period, a total of \$99,579.91 was received as deposits (credits) into the account, and \$95,356.61 was withdrawn.

44. The percentage breakdown of the received deposits into Account #6198 are: Cash Deposits: 75.88%, Check Deposits: 0.51%, Money Order Deposits: 9.96% and Other Deposit: 13.65%. The majority of the withdrawals were counter checks made payable to SIMON or cash, for a total of \$40,788. An additional \$15,944.56 was withdrawn via ATM and \$38,544.76 spent on what appear to be personal expenses. Thus, cash was the majority of flow in and out of the account, which your affiant knows is commonly used in fraud schemes due to the limited trackability of cash. The majority of victim's fraudulently used bank cards were used for ATM cash withdrawals or money order purchases, which was routine activity for Account #6198.

45. The second and third accounts in SIMON's name were with Bank of America (Checking Account # 0264 and Savings Account #0309). The USSS obtained records for Account #0264 from May 2016 through July 2016. Over the analysis period, a total of \$16,361.10 was received as deposits (credits) into the account and the exact same amount was withdrawn.

46. The percentage breakdown of the received deposits into Account #0264 are: ATM Deposits: 86.67%, Transfer-in: 6.11%, Cash Deposit: 5.71%, and Misc. Deposit: 1.50%. Much like the pattern of the abovementioned BB&T account, cash and ATM deposits are the majority of money flow in and out of the account.

RECENT CRIMINAL ACTIVITY

47. I believe that SIMON has continued with the criminal scheme. Although activity slowed following execution of the search warrant, the same pattern has been occurring more and more often since April 2020. Between the dates of April 20, 2020 and April 29, 2020 a new phone number, Phone 1542, called four (4) confirmed victims. With


each call, a female bank representative called the victim notifying them of compromised bank cards. Subsequently, a bank representative collected bank cards from the victims and fraudulent charges were made.

48. In one incident on April 21, 2020, victim "L.B." received a call from Phone 1542, and subsequently handed over bank cards to a bank representative that arrived at L.B.'s house. Approximately \$4,000 worth of fraudulent purchases and ATM withdrawals were made on L.B.'s BofA accounts. BofA captured Phone 1542 calling the customer service line on April 21, 2020, requesting the ATM withdrawal limits to be increased on L.B.'s account. This call was recorded. A PBSO detective had previously reviewed SIMON's voice on captured calls from bank recordings, including after the CD identified SIMON's voice. The PBSO detective recognized SIMON's voice as the caller on the BoA customer service line on April 21, 2020.

49. Historical cell-site records for Phone 1542 show that the phone was located approximately 25 miles southwest of Atlanta, Georgia. This general location is near SIMON's HOUSE where the USSS executed the search warrant.

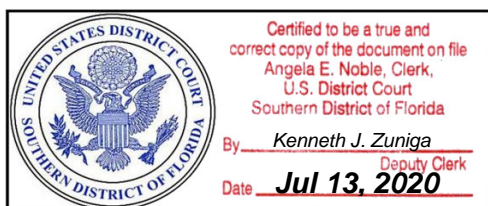
50. Based on the continued scheme with the elderly being targeted, a female bank representative calling the victims, and SIMON's voice identified on a captured bank phone call, I believe that SIMON has continued to orchestrate this scheme following her residence being searched on February 5, 2020.

FURTHER YOUR AFFIANT SAYETH NAUGHT.



Sarah Schaut
Task Force Officer
United States Secret Service

Sworn and Attested to me by Applicant by Telephone (FaceTime) per Fed.R.Crim.P. 4(d) and 4.1, in West Palm Beach, Florida, on July 13, 2020.





WILLIAM MATTHEWMAN
UNITED STATES MAGISTRATE JUDGE