

AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

Western District of Texas

United States of America
v.
OLUMIDE BANKOLE MORAKINYO

Case No. 1:19-MJ-397-AWA
FILED

JUL 19 2019

Defendant(s)

CRIMINAL COMPLAINT

CLERK, U.S. DISTRICT COURT
WESTERN DISTRICT OF TEXAS
BY [Signature] DEPUTY CLERK

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 May 1, 2017 in the county of Travis in the
Western District of Texas, the defendant(s) violated:

Code Section

Offense Description

Title 18 USC 1956(h)

-Conspiracy to commit money laundering

This criminal complaint is based on these facts:

See Attachment

[X] Continued on the attached sheet.

[Signature of Cade Cannon]
Complainant's signature

Cade Cannon, FBI Special Agent

Printed name and title

Sworn to before me and signed in my presence.

Date: 7/19/2019

[Signature of Andrew W Austin]
Judge's signature

City and state: Austin, Texas

Andrew W Austin, US Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF TEXAS
AUSTIN DIVISION

AFFIDAVIT IN SUPPORT OF COMPLAINT

I, Cade Cannon, being first duly sworn, hereby state as follows:

I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been employed as a Special Agent since October 10, 2010. After completing FBI New Agent Training in Quantico, Virginia, I was initially assigned to the Miami Field Office where I investigated fraud and money laundering crimes for approximately three years. Two of these investigations proceeded to trial where I testified extensively regarding fraud and money laundering crimes. In this capacity, I also received training related to fraud and money laundering crimes. I am currently assigned to the San Antonio Division, Austin Resident Agency, where I investigate computer intrusion matters. In this capacity, I have received training and have experience in conducting investigations related to computer crimes, including fraud.

This affidavit is intended to show merely that there is sufficient probable cause for the requested Complaint and Arrest Warrant. It does not set forth all of my knowledge about this matter. All facts are relayed in sum and substance.

Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1956(h) (money laundering conspiracy) have been committed by **Olumide Bankole Morakinyo**.

THE STATUTE VIOLATED

Title 18 U.S.C. 1956, Money Laundering:

“(a)(1)Whoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial transaction which in fact involves the proceeds of specified unlawful activity—

(A) (i) with the intent to promote the carrying on of specified unlawful activity; or

(B) knowing that the transaction is designed in whole or in part—

(i) to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity; or

(ii) to avoid a transaction reporting requirement under State or Federal law,

shall be sentenced to a fine of not more than \$500,000 or twice the value of the property involved in the transaction, whichever is greater, or imprisonment for not more than twenty years, or both. For purposes of this paragraph, a financial transaction shall be considered to be one involving the proceeds of specified unlawful activity if it is part of a set of parallel or dependent transactions, any one of which involves the proceeds of specified unlawful activity, and all of which are part of a single plan or arrangement.

(h) Any person who conspires to commit any offense defined in this section or section 1957 shall be subject to the same penalties as those prescribed for the offense the commission of which was the object of the conspiracy.”

FACTS ESTABLISHING PROBABLE CAUSE

Summary

Olumide Morakinyo (Morakinyo), a Canadian resident, former resident of the United States, and native of Nigeria, conspired with others, including Lukman Aminu (Aminu), to commit money laundering. Morakinyo used Aminu to procure prepaid debit cards in the United States; Aminu would then send Morakinyo the debit card numbers. Those cards were then

activated with the personally identifiable information (“PII”) of victim of multiple scams. Money was taken from or in the name of those victims and then loaded onto those cards. Aminu, who still possessed the physical cards, would then withdraw the money under instructions from Morakinyo. Aminu would then transfer or deposit that money at Morakinyo’s direction. As described below, two of the scams victimized individuals in the Western District of Texas. One scam involved defrauding the Employees Retirement System of Texas; the other scam involved stealing the PII from a Texas Certified Public Accountant (CPA) and filing fraudulent tax refunds with the Internal Revenue Service.

Detailed Facts

Beginning in June of 2017, an unidentified subject, or subjects, began creating unauthorized accounts for participants in the Employees Retirement System of Texas (“ERS”) internet portal. The subject accessed the ERS participant internet portal and used ERS participants’ PII to create 30 accounts for participants who were all over the age of 65 and did not have accounts in the portal. After creating the accounts, the subject changed the bank accounts on file with ERS for 26 participants’ retirement payments. ERS, based in Austin, Texas, in the Western District of Texas, detected the fraudulent activity, but not before ERS sustained an actual loss of \$10,605.18 with a potential minimum attempted loss estimated at \$131,461.64.

On July 31, 2017, an unidentified subject created an account for Victim-1 in the ERS internet portal using Victim-1’s PII. The subject then successfully changed the bank account on file with ERS for Victim-1 to a MasterCard prepaid debit card issued by Green Dot Bank (the “Green Dot card”). On August 29, 2017, Victim-1’s monthly retirement payment of \$1,972.97

was deposited onto the Green Dot card. On September 27, 2017, Victim-1's monthly retirement payment of \$1,972.97 was again deposited onto the Green Dot card.

According to Green Dot account records, Victim-2, a resident of West Orange, New Jersey, activated the Green Dot card on June 27, 2017. On February 8, 2018, Victim-2, 82 years old, was interviewed by law enforcement and stated she had never purchased, owned, or received a Green Dot prepaid debit card. Victim-2 also stated that at some point in 2017 she did not receive her deceased husband's monthly retirement payment of \$1,561.22 from Prudential Financial. Records subpoenaed from Green Dot showed a payment of \$1,561.22 on July 31, 2017, from Prudential to the Green Dot card.

Records provided by Green Dot showed that the Internet Protocol address 45.76.175.244 was used numerous times from July 31, 2017 through October 17, 2017, to access the online account for the Green Dot card. An Information Security Officer employed at ERS confirmed that this IP address, 45.76.175.244, was also used to access the ERS participant internet portal on October 7, 2017, and October 9, 2017. Unauthorized accounts were created in the ERS participant internet portal on both of these days. The IP address is registered to Choopa, LLC, a company that provides "bulletproof hosting" to customers who wish to obtain IP addresses anonymously.

An analysis of records showed that on August 30, 2017, the day after Victim-1's retirement payment was deposited on the Green Dot card, the card was used at a Hannaford Supermarket in Manchester, NH, to make a purchase of \$1,904. Records also showed that on September, 28, 2017, the day after Victim-1's second retirement payment was deposited on the Green Dot card, the card was again used at a Hannaford in Manchester, NH, to make a purchase of \$1,905.

Records subpoenaed from Hannaford Supermarket showed that the purchases were of Western Union money orders. Two of the \$500 money orders were made out to "Lukman Aminu." Hannaford also provided photographs of the individual who purchased the money orders on September 28, 2017 and it appears to show Aminu. The MoneyGram money order payable to Aminu was deposited into an account at Digital Federal Credit Union. Account records showed that Aminu opened the account on March 16, 2016, and provided the email address engineerlookman@yahoo.com in the account application. The account was closed on November 6, 2017. On May 28, 2018, a search warrant was executed on the email account engineerlookman@yahoo.com. A review of the emails showed the account was used to send credit card numbers with expiration dates and CCV numbers to marvinalba247@yahoo.com. The search warrant returns from Yahoo included emails sent and received by a second Yahoo email account, edwardheaton999@yahoo.com. The Yahoo representative explained that edwardheaton999@yahoo.com was an Internet Message Access Protocol email account linked to engineerlookman@yahoo.com.

On July 19, 2018, a search warrant was executed on the email account edwardheaton999@yahoo.com. A review of the account showed the edwardheaton999@yahoo.com account was used to send emails containing bank account information (including account usernames and passwords) and credit card numbers (with expiration dates and CCV numbers) to multiple email accounts.

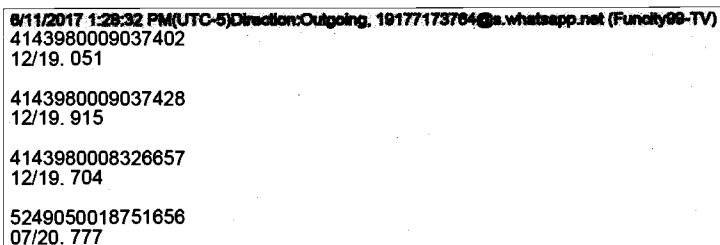
On July 12, 2018, Aminu was arrested pursuant to a complaint issued in the Western District of Texas charging him with Conspiracy to Commit Money Laundering for his role in the ERS fraud. Aminu agreed to speak with law enforcement following his arrest. During the interview, Aminu admitted he used an email account, edwardheaton999@yahoo.com, at the

direction of an associate, Olumide Morakinyo, to send Morakinyo numbers for prepaid debit cards issued by Green Dot that Aminu purchased in New Hampshire. Morakinyo would then load money onto the prepaid debit cards and email the numbers back to Aminu once they were loaded. Aminu would then withdraw the money from the cards.

Following Aminu's arrest, a search warrant was executed at his residence and on his electronic devices, including his mobile phone. A review of Aminu's WhatsApp account on his mobile phone showed messages between Aminu and a contact named "Olu Cana." The phone number associated with "Olu Cana" was (226) 606-7625, a Canadian number. From May 1, 2017, to June 28, 2018, Aminu sent messages to "Olu Cana" with the numbers of approximately 300 MasterCard prepaid debit cards issued by Green Dot.

On June 11, 2017 Aminu sent a WhatsApp message to "Olu Cana," phone number (226) 606-7625, with the account information for the Green Dot card that was used to receive Victim-1's ERS retirement payments. On August 30, 2017, "Olu Cana" sent Aminu a WhatsApp message that read "1656 abere 8532 elo 1972." 1656 are the last four digits of the Green Dot card used to receive Victim-1's ERS retirement payments. \$1,972.97 is the amount of Victim-1's ERS retirement payment that was deposited on the Green Dot card on August 31, 2017.

Figure 1 – Screenshot of 06/11/2017 WhatsApp Message from Lukman Aminu to "Olu Cana"



6/11/2017 1:28:32 PM(UTC-5)Direction:Outgoing, 19177173704@.whatsapp.net (Funcity08-TV)
4143980009037402
12/19. 051

4143980009037428
12/19. 915

4143980008326657
12/19. 704

5249050018751656
07/20. 777

*Figure 2 – Screenshot of 08/30/2017 WhatsApp Messages between “Olu Cana” and Lukman**Aminu*

<p>8/30/2017 11:18:16 AM(UTC-5)Direction:Incoming, 1228667625@.whatsapp.net (Olu Cana) 1656 abere 8532 elo 1972</p> <p>Platform: Mobile</p>
<p>8/30/2017 11:18:32 AM(UTC-5)Direction:Outgoing, 10177173764@.whatsapp.net (Funday99-TV) Ok</p> <p>Status: Sent Platform: Mobile</p>

A subpoena was issued to Green Dot for records related to the Green Dot prepaid debit cards sent by Aminu to “Olu Cana” through WhatsApp. In addition to the Green Dot card used to receive the Victim-1’s ERS retirement payments, 254 additional Green Dot cards sent by Aminu to “Olu Cana” were registered with different individuals’ personally identifiable information. Approximately \$265,000 was loaded on 47 of these cards. Approximately \$229,000 of this total amount came from deposits by the U.S. Internal Revenue Service. Three of the deposits by the U.S. Internal Revenue Service were made on Green Dot cards registered in the names of clients of an accounting firm in Georgetown, Texas, which is within the Western District of Texas. The owner of the firm, a certified public accountant, was interviewed by law enforcement and confirmed that fraudulent tax filings had been made for a number of his clients in 2017. After the fraudulent tax filings were discovered, a forensic investigation determined the firm’s computer system had been infected with malware.

A subsequent review of Aminu’s WhatsApp messages with “Olu Cana” showed that on May 1, 2017, Aminu sent a WhatsApp message to “Olu Cana” with nine Green Dot card numbers, including one with 7971 as the last four digits. On May 16, 2017, “Olu Cana” sent Aminu a WhatsApp message that read “017971 abere 2131 amt 8160.” Subpoenaed records showed that the Green Dot card ending in 7971 was registered in the name of Victim-3, a client

of the accounting firm in Georgetown, Texas. Victim-3's tax refund for \$8,490 was deposited on the card.

Figure 3 – Screenshot of 05/01/2017 WhatsApp Message from Lukman Aminu to “Olu Cana”

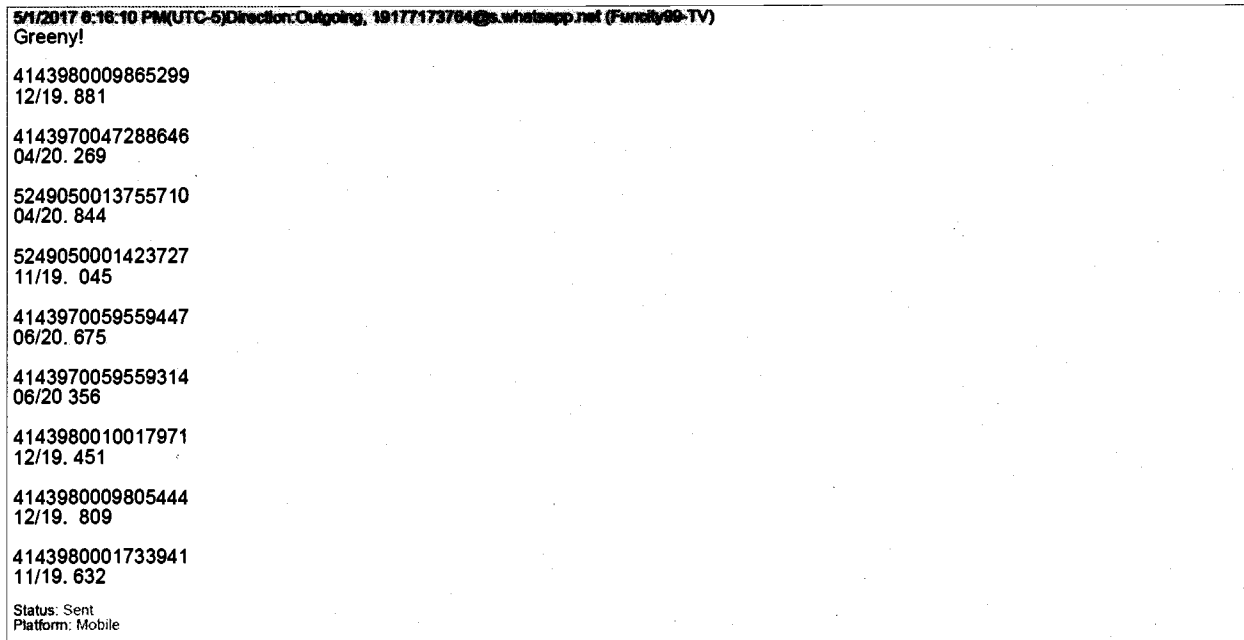
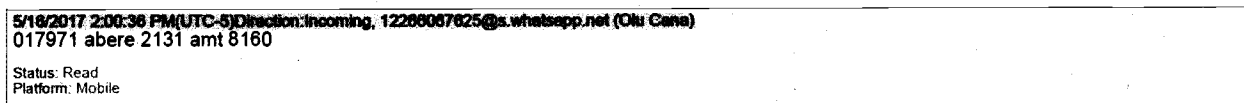
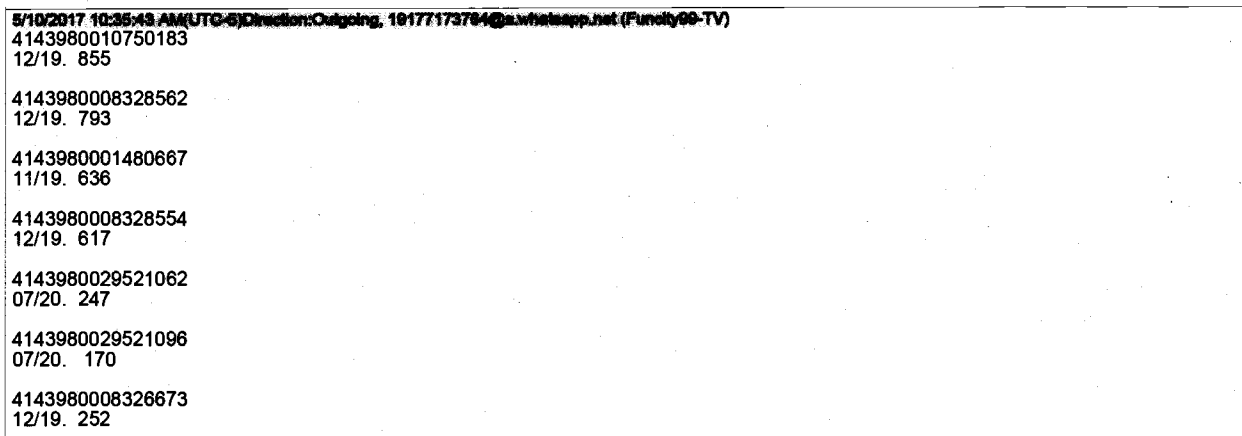


Figure 4 – Screenshot of 05/16/2017 WhatsApp Message from “Olu Cana” to Lukman Aminu



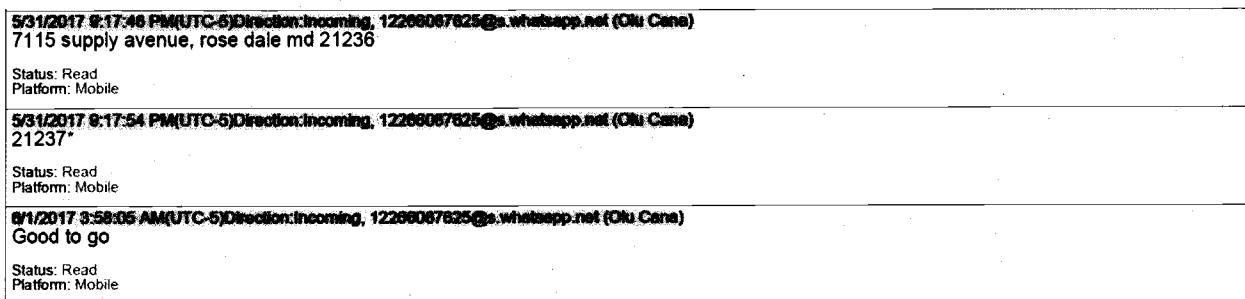
On May 10, 2017, Aminu sent a WhatsApp message to “Olu Cana” with seventeen Green Dot card numbers including one with 1096 as the last four digits and another with 6673 as the last four digits. Subpoenaed records showed that the Green Dot card ending in 1096 was registered in the name of Victim-4, a client of the accounting firm in Georgetown, Texas. IRS records show that Victim-4's tax refund for \$4,236 was issued and directed to the Green Dot card. Subpoenaed records showed that the Green Dot card ending in 6673 was registered in the name of Victim-5, also a client of the accounting firm in Georgetown, Texas. Victim-5's tax refund for \$8,886.37 was issued and directed to the Green Dot card.

Figure 5 – Screenshot of 05/10/2017 WhatsApp Message from Lukman Aminu to “Olu Cana”



On May 31, 2017, “Olu Cana” sent Aminu a WhatsApp message with the address “7115 supply avenue, rose dale, md 21236.” “Olu Cana” sent a subsequent message that read “21237*.” 21237 is the correct zip code for 7115 Supply Avenue, Rosedale, Maryland. After sending the address, “Olu Cana” sent Aminu a third message that read “Good to go.”

Figure 6 – Screenshot of 05/31/2017 WhatsApp Message from “Olu Cana” to Lukman Aminu



On June 9, 2017, “Olu Cana” sent Aminu a WhatsApp message that contained a photo of a Barclays Bank credit card in the name of Victim-6. A subpoena was issued for records related to the credit card. The Barclays Bank records indicated an unidentified individual applied for a Barclaycard MasterCard on June 1, 2017, in the name of Victim-6. Stolen personal identifying information (PII) for Victim-6, to include his date of birth and social security number, was used in the application for the credit card. The application was approved, and Barclays Bank credit

card number 5199-5500-0590-2121 was issued and sent to the home address on the application, 7115 Supply Avenue, Rosedale, Maryland, 21237. On March 1, 2019, Victim-6 was interviewed by the FBI and stated he had never had a Barclays Bank credit card.

Records provided by Barclays Bank showed that the credit card was used during a two-week period in June and July of 2018, to make \$8,407.00 in purchases at various restaurants, retail stores, and grocery stores in the Toronto and Ottawa, Canada, metro areas. The credit card was also used to make \$3,837.21 in cash advances at the TD Bank branch in Brampton, Ontario, Canada. Barclays never received any payments for this account and the account was closed for non-payment. Barclays Bank confirmed to Texas DPS that the bank charged off an outstanding balance on the credit card of \$14,323.68, which includes the original charges of \$12,244.21 plus interest and outstanding late fees.

The address used on the credit card application, 7115 Supply Avenue, Rosedale, Maryland, 21237, is located in an industrial park in the Baltimore metro area. Olumide Morakinyo, a current resident of Ontario, Canada, is associated with the 7115 Supply Avenue address in law enforcement databases and used the address for a personal Bank of America Bank account as late as November of 2018.

Figure 7 – Screenshot of 06/09/2017 WhatsApp Messages between Lukman Aminu and “Olu Cana”



<p>06/2017 10:09:12 PM(UTC-5)Direction:Outgoing, 19177173764@s.whatsapp.net (Funchy99-TV) Make victor snap front n back for us nah</p> <p>Status: Sent Platform: Mobile</p>
<p>06/2017 10:09:14 PM(UTC-5)Direction:Outgoing, 19177173764@s.whatsapp.net (Funchy99-TV) Chai</p> <p>Status: Sent Platform: Mobile</p>
<p>06/2017 10:09:36 PM(UTC-5)Direction:Incoming, 1226067625@s.whatsapp.net (Olu Cana) I Don tell am so</p> <p>Status: Read Platform: Mobile</p>
<p>06/2017 10:09:45 PM(UTC-5)Direction:Outgoing, 19177173764@s.whatsapp.net (Funchy99-TV) He don kolo</p> <p>Status: Sent Platform: Mobile</p>
<p>06/2017 10:41:57 PM(UTC-5)Direction:Incoming, 1226067625@s.whatsapp.net (Olu Cana)</p> <p>Attachments:</p>  <p>https://mmg.whatsapp.net/d/f/AnUjI-X9yUDxA_ApBubvutij6cHQQuayCj3ACmOrDyqg.enc 70f4a25d-89fb-4bd9-92bd-dabf72a1153b.jpg</p> <p>Status: Read Platform: Mobile</p>
<p>06/2017 10:41:57 PM(UTC-5)Direction:Incoming, 1226067625@s.whatsapp.net (Olu Cana)</p> <p>Attachments:</p>  <p>https://mmg.whatsapp.net/d/f/AufdowK1B9fDSZpAHO LnBEvHA16jzZDOWCmjK-VFcup8.enc d9963d1c-ad8c-4313-923f-0c605d89aae5.jpg</p> <p>Status: Read Platform: Mobile</p>

Figure 8 – Photo from 06/09/2017 WhatsApp Messages between Lukman Aminu and “Olu Cana”



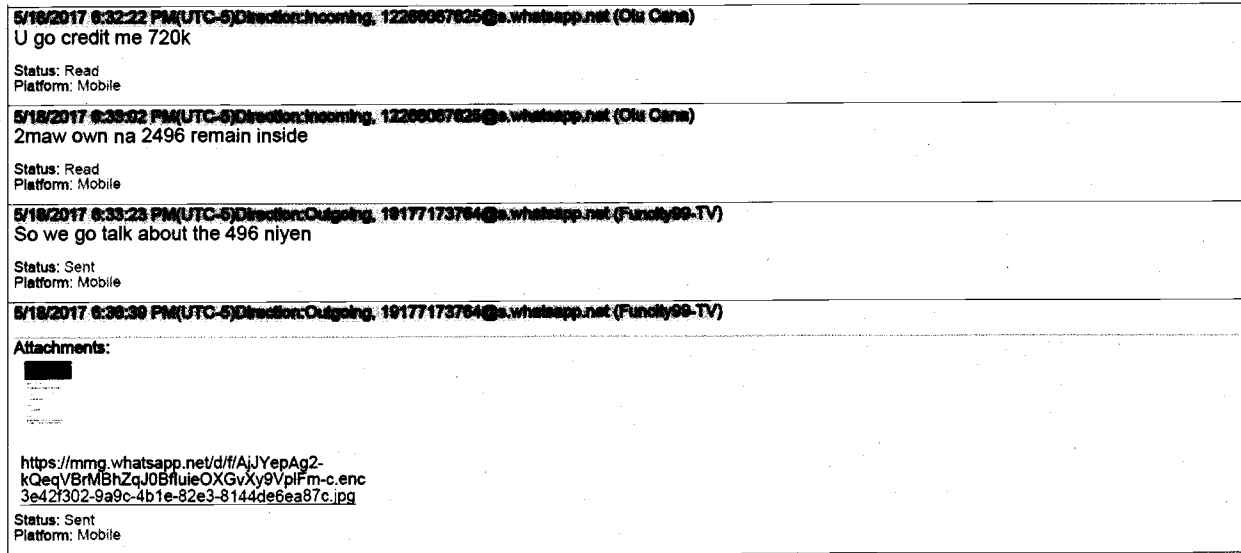
On August 21, 2018, Aminu was indicted by a Grand Jury in the Western District of Texas (1:18-cr-328-RP) for conspiracy to commit money laundering and aggravated identity theft. On January 2, 2019, Aminu entered a guilty plea to one count of conspiracy to commit money laundering related to the scheme described in this Affidavit. Aminu later pleaded guilty to receipt of stolen property as part of his role in an unrelated scheme. Aminu is cooperating with law enforcement in hopes of consideration at sentencing.

A subpoena was issued to WhatsApp for information related to the account associated with the phone number for "Olu Cana," (226) 606-7625. WhatsApp provided "Device Info" for the account as "os: 6.0, model: HTC htc_m8." Based on a review of HTC's website, www.HTC.com, HTC is a manufacturer of cell phones and HTC ONE M8 is a model of cell phone manufactured by the company.

The phone number (226) 606-7625 also appeared in records subpoenaed from MoneyGram for transactions related to Aminu. Morakinyo sent nine MoneyGram money orders to Aminu that included Morakinyo's name, an address in Ontario, Canada, and the phone number for "Olu Cana," (226) 606-7625. Morakinyo also provided this same Ontario, Canada, address and phone number, (226) 606-7625, on a U.S. immigration form, a DS-160 visa application, submitted to the U.S. government on January 1, 2016.

On U.S. immigration forms, Morakinyo listed his spouse as Isioma Isamah. On May 18, 2017, "Olu Cana" sent Aminu a message that read "U go credit me 720k." Aminu then sent "Olu Cana" a message with an attachment showing an "Account Transfer from AMINU, LUKMAN to ISIOMA ISAMAH" totaling 1,000,000 Nigerian Naira.

Figure 9 – Photo from 05/18/2017 WhatsApp Messages between Lukman Aminu and “Olu Cana”



When interviewed, Aminu confirmed that “Olu Cana,” the user of (226) 606-7625, was Olumide Morakinyo, a resident of Ontario, Canada. In addition to their WhatsApp communications, phone records indicate the two were in frequent telephonic communication. Aminu stated that he initially met Morakinyo in 2015 when both Aminu and Morakinyo were living near Baltimore, Maryland. While living in Maryland, Aminu began helping Morakinyo withdraw money from Green Dot cards. At some point, Morakinyo and Aminu had a dispute and Aminu stopped working with him. Morakinyo moved from Maryland to Canada and Aminu moved to New Hampshire. After living and working in Manchester, New Hampshire, for a period of time, Aminu lost his job and began working for Morakinyo again. Aminu stated that Morakinyo would send the Green Dot card numbers provided by Aminu to “Additional Suspect 1” (name withheld for investigative reasons) who was a member of a group in Nigeria that conducted fraud. Additional Suspect 1 would load the Green Dot cards with money and Morakinyo then helped the group obtain the proceeds of the fraud. The WhatsApp messages between Aminu and Morakinyo, along with the email messages between Aminu and email

addresses he said belonged to Morakinyo, support Aminu's description of the money laundering scheme he engaged in with Morakinyo.

On December 21, 2019, a search warrant was obtained for a Facebook account belonging to Morakinyo (1:18-mj-787-ML). The "Registration Date" for the account is listed as August 17, 2007. Two of the "Registered Email Addresses" for the Facebook account were snazzyolu@gmail.com and snazzyolu@yahoo.com. A review of the contents of the Facebook account showed a conversation between Morakinyo and Facebook user Kaomi Smart. On March 2, 2018, Morakinyo stated "go update u soon on our level." On March 9, 2018, Smart sent Morakinyo a message stating: "How far brother I never hear from you about the level and I broke right now if u could sort me out asap I'll appreciate it a lot." I know from experience and discussions with other law enforcement that the term "level" is used by individuals involved in computer crime to refer to fraudulent schemes.

In a 2015 application for a United States B1/B2 Visa, Morakinyo provided the email account, olumide@morakinyo.com, as his email account. On February 12, 2019, a search warrant was executed on the account (1:19-mj-62-ML). The search warrant response provided by Microsoft listed the "Device User Agent" associated with the account as "HTC-EAS-HTCOneM8." The account contained approximately 100 emails that were sent from olumide@morakinyo.com to the email account snazzyolu@gmail.com. The account also contained approximately 80 messages that were sent to the email account moraksolu@yahoo.com from May 12, 2017, to May 19, 2018.

On March 19, 2019, a search warrant was executed on the account snazzyolu@gmail.com (1:19-mj-107-ML). The search warrant response provided by Google listed "Device Attributes" for the email account, to include "Model: HTC One_M8." The "Recovery e-Mail" for the

account was listed as account moraksolu@yahoo.com. The account also contained five messages that were received from the account moraksolu@yahoo.com from December 29, 2017 to January 14, 2019. Morakinyo also provided the email account moraksolu@yahoo.com as his email account on a 2010 application for a United States B1/B2 Visa.

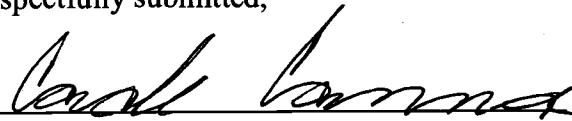
Many of the emails in the Microsoft and Google accounts contained information related to the purchase of used cars in the U.S. for shipment to Nigeria. This is a common method used by individuals involved in computer crime to launder the proceeds of crime.

On June 28, 2019, U.S. Customs and Border Protection confirmed that Morakinyo crossed from Canada into the U.S. at Lewiston, New York. Morakinyo entered the U.S. with his spouse, Isioma Isamah, and two minors. Canadian law enforcement confirmed that Morakinyo crossed back into Canada from the U.S. on July 1, 2019.

REQUEST FOR SEALING

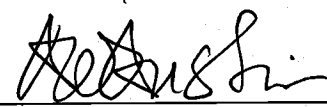
I further request that the Court order that all papers in support of this application, including the affidavit and criminal complaint, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, involving undercover activity and covert operations, which is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



Cade Cannon
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me on July 19, 2019.



HONORABLE ANDREW W. AUSTIN
UNITED STATES MAGISTRATE JUDGE
WESTERN DISTRICT OF TEXAS