

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY



UNITED STATES OF AMERICA	:	Hon. Leda D. Wettre
	:	
v.	:	Mag. No. 18-8111
	:	
AKINTUNDE ADEYEMI,	:	<u>CRIMINAL COMPLAINT</u>
a/k/a "AK," and	:	
OLUWASEUN JATO	:	

I, Ryan Orr, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Postal Inspector with the United States Postal Inspection Service, and that this complaint is based on the following facts:

SEE ATTACHMENT B

Continued on the attached page and made a part hereof:

Ryan Orr
Postal Inspector
United States Postal Inspection Service

Sworn to before me and subscribed in my presence,
July 17, 2018 in Essex County, New Jersey

HONORABLE LEDA D. WETTRE
UNITED STATES MAGISTRATE JUDGE

Leda Dunn Wettre

Signature of Judicial Officer

ATTACHMENT A

Count One
(Conspiracy to Commit Bank Fraud)

From at least as early as in or around July 2016 through in or around May 2017, in the District of New Jersey, and elsewhere, the defendants,

AKINTUNDE ADEYEMI,
a/k/a "AK," and
OLUWASEUN JATO

did knowingly and intentionally conspire and agree with each other and others to execute a scheme and artifice to defraud financial institutions, as defined in Title 18, United States Code, Section 20, whose deposits were insured by the Federal Deposit Insurance Corporation, and to obtain monies, funds, assets, and other property owned by and under the custody and control of such financial institutions, by means of materially false and fraudulent pretenses, representations, and promises, contrary to Title 18, United States Code, Section 1344.

In violation of Title 18, United States Code, Section 1349.

Count Two
(Aggravated Identity Theft)

On or about August 31, 2016, in the District of New Jersey, and elsewhere,
the defendant,

AKINTUNDE ADEYEMI,
a/k/a "AK"

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another individual, namely a credit card account of Victim Cardholder 1, during and in relation to a felony violation of a provision contained in Chapter 63 of the United States Code, that is, conspiracy to commit bank fraud in violation of Title 18, United States Code, Section 1349, charged in Count One of this Criminal Complaint.

In violation of Title 18, United States Code, Section 1028A(a)(1), and Title 18, United States Code, Section 2.

Count Three
(Aggravated Identity Theft)

On or about April 8, 2017, in the District of New Jersey, and elsewhere,
the defendant,

OLUWASEUN JATO

did knowingly transfer, possess, and use, without lawful authority, a means of identification of another individual, namely a credit card account of Victim Cardholder 2, during and in relation to a felony violation of a provision contained in Chapter 63 of the United States Code, that is, conspiracy to commit bank fraud in violation of Title 18, United States Code, Section 1349, charged in Count One of this Criminal Complaint.

In violation of Title 18, United States Code, Section 1028A(a)(1), and Title 18, United States Code, Section 2.

ATTACHMENT B

I, Ryan Orr, am a Postal Inspector with the United States Postal Inspection Service. I have knowledge about the facts set forth below from my involvement in the investigation, my review of reports, documents, pictures, videos, witness interviews, and discussions with other law enforcement officials. Because this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact that I know concerning this investigation. All statements described in this Criminal Complaint are relayed in substance and in part. In addition, where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

Relevant Individuals and Entities

1. At various times relevant to this Criminal Complaint:
 - a. Defendant AKINTUNDE ADEYEMI, a/k/a “AK” (“**ADEYEMI**”), was a resident of East Orange, New Jersey and Duluth, Georgia.
 - b. Defendant OLUWASEUN JATO (“**JATO**”) was a resident of Newark, New Jersey.
 - c. “Victim Bank 1” was a “financial institution” as that term is defined in Title 18, United States Code, Section 20, offering, among other things, credit cards to customers.
 - d. “Victim Cardholder 1” was a customer of Victim Bank 1 who resided in or around Jacksonville, Florida, and held a credit card account ending in account number 8831.
 - e. “Victim Cardholder 2” was a customer of Victim Bank 1 who resided in or around East Grand Rapids, Michigan, and held a credit card account ending in account number 5209.

Overview of the Conspiracy

2. Beginning at least as early as in or around July 2016 through in or around May 2017, defendants **ADEYEMI**, **JATO** and others conspired to obtain control of credit card accounts using stolen personal identifying information (“PII”) of third parties. Specifically, **ADEYEMI**, **JATO** and other co-conspirators submitted to Victim Bank 1 applications for credit card accounts using stolen PII, including the names, addresses, and other identifying information of the unsuspecting identity theft victims. After establishing the accounts, the co-conspirators contacted Victim Bank 1 to change the address associated with

the accounts so that Victim Bank 1 would send the credit cards to those addresses. The co-conspirators then monitored those addresses and intercepted the cards before the residents of the addresses received them. Some of these addresses were located near the defendants' residences in New Jersey and Georgia. The co-conspirators then used the cards at retail stores in New Jersey and Georgia, among other places, to purchase smartphones, tablets, and other high-value items, which they then sold for profits. Through these methods, the co-conspirators defrauded Victim Bank 1 of over \$600,000.

Defendants' Participation in the Conspiracy

3. Defendants **ADEYEMI** and **JATO** have been linked to various stages of the scheme, including distributing stolen PII and compromised credit card account information, making high-value purchases with the compromised accounts, and moving criminal proceeds both domestically and internationally. The investigation has revealed that **ADEYEMI** and **JATO** held unique roles in the scheme. **ADEYEMI** obtained the stolen PII from other co-conspirators and used it to create the fraudulent credit card accounts. He then sent the account information to others, including **JATO**, who coordinated with other co-conspirators to retrieve the credit cards associated with the compromised accounts. **JATO** and other co-conspirators then used the cards to make retail purchases.

4. Victim Bank 1 identified the compromised accounts associated with the scheme (the "Compromised Accounts") through several common characteristics, including: the telephone number used to contact Victim Bank 1 to change the address on the account or to take other action relating to the account; the IP address from which the fraudulent account application was submitted; and the domain name of the email address listed on the application. Evidence developed in the investigation reveals numerous connections between **ADEYEMI** and **JATO** and the Compromised Accounts.

A. The Adeyemi Domains and Email Accounts

5. Many of the applications for the Compromised Accounts listed email addresses with the domain names "Southwildlife.com," "Ultramilesclub.com," and "Andconsul.com" (the "Subject Domains"). Law enforcement discovered numerous emails associated with these domains in an email account used by **ADEYEMI** ("Adeyemi Email Account 1"), including email communications from Victim Bank 1 relating to certain Compromised Accounts. Moreover, registration records relating to the Southwildlife.com domain list Adeyemi Email Account 1 as the email account associated with the registration. In addition to Adeyemi Email Account 1, law enforcement has identified two other email accounts **ADEYEMI** used to facilitate the scheme ("Adeyemi Email Accounts 2 and 3").

6. Law enforcement has determined that **ADEYEMI** uses the Adeyemi Email Accounts. Specifically, agents have reviewed chat communications discovered in the Adeyemi Email Accounts in which the user is referred to as "AK," **ADEYEMI**'s principal alias, or "Saintaklo," another alias **ADEYEMI** has used. In one chat, **ADEYEMI** stated,¹ "i used to have this ID saintaklo," "[I] just came back online after almost 3 years," "I did 32 months, money laundry and credit card fraud .. but i am good[.]" Notably, in or around October 2015, **ADEYEMI** was convicted in the Superior Court of New Jersey in connection with a credit card fraud scheme and was sentenced to approximately 2.5 years in prison. **ADEYEMI** likely was referring to that conviction and sentence in this chat. Later in the chat, he stated, "[I] want to get back to work[,] 32 months can't stop me man." Moreover, agents discovered travel itinerary in **ADEYEMI**'s full name in one of the Adeyemi Email Accounts. Agents also discovered photographs of an individual matching the general appearance of **ADEYEMI** in one of the Adeyemi Email Accounts. Last, as described further below, **ADEYEMI** acknowledged using at least one of the Adeyemi Email Accounts in a consensually recorded call with a cooperating witness.

7. Law enforcement has reviewed communications from the Adeyemi Email Accounts in which **ADEYEMI** discussed with other co-conspirators account information relating to Compromised Accounts, including the name and account number associated with the accounts. For example, in an online chat on or about August 31, 2016, a co-conspirator not charged as a defendant herein ("CC#1") sent **ADEYEMI** the account number, expiration date, security code and cardholder name associated with a credit account provided by Victim Bank 1. The PII associated with this Compromised Account belonged to Victim Cardholder 1. In the chat, CC#1 asked **ADEYEMI** how to use the Compromised Account, and **ADEYEMI** indicated in response that he was about to activate the account, stating, "I don dey activate the cards...gimme 5 minutes."

8. Similarly, on or about July 3, 2016, **ADEYEMI** engaged in an online chat with another co-conspirator not charged as a defendant herein ("CC#2") during which **ADEYEMI** provided guidance on changing the address associated with a Compromised Account. The following chat took place:

CC#2: yes bro

ADEYEMI: nice one

ADEYEMI: i no dey like mentioning real names on chats[.]

¹ Any chat or email communications quoted in this complaint are set forth verbatim without correcting typographical or other errors.

CC#2: Oh okay ...

CC#2: AK is there any job update i fit work on

ADEYEMI: bro no dey mention AK on chat jare

CC#2: Oh oh ...

CC#2: Sorry ... got you now

ADEYEMI: na [Victim Bank 1] i dey do mainly sha

ADEYEMI: i dont reall do much.. just [Victim Bank 1]

CC#2: en en...na appluy

ADEYEMI: yes.. apply

ADEYEMI: apply to previous address wey dey on credit history

ADEYEMI: then call after 8 days ,, to change address and replace the card.. dem go ask security questions and background search questions and after that he go go .. i will tell dem to expedite the shipping so he go deliver next day

CC#2: oh okay..

CC#2: thanks bro

Based on the context of this and other communications reviewed in the investigation, **ADEYEMI** likely was telling CC#2 how to change the address associated with a Compromised Account so that Victim Bank 1 would send a replacement card that the co-conspirators would intercept and use in furtherance of the scheme.

9. In addition to providing to co-conspirators account information for Compromised Accounts, **ADEYEMI** also assisted co-conspirators in creating fake identification cards in the names of the victim account holders, which the co-conspirators could use if required when making retail purchases. **ADEYEMI** discussed these fake identification cards in email communications sent through Adeyemi Email Account 1. For example, on or about September 18, 2016, **ADEYEMI** sent an email to a co-conspirator not charged as a

defendant herein ("CC#3"). The subject line of the email was "This is how the ID will look after you finish it." The email attached a file named "Original Mississippi" that contained photos of a Mississippi driver's license in the name of a third-party who appears to be a victim of identity theft ("Individual 1"). The email stated: "The name of this ID is: [Individual 1], if you look the ID well you will notice the last name comes first then comma sign, then the first name. Then you will notice the signatures across the 2 pictures on the ID have the name [Individual 1] written on them in signature form.. Pls take you time to study the sample pictures ... That exactly how I want the IDs to be.."

10. **ADEYEMI** sent CC#3 similar emails in March 2017 using Adeyemi Email Account 1. Specifically, on or about March 1, 2017, **ADEYEMI** sent CC#3 an email with the subject line "Info for ID 3." The body of the email listed the name, address, height, weight, sex, and date of birth for an individual residing in Missouri ("Individual 2"). Victim Bank 1 has advised law enforcement that, on or about February 16, 2017, a fraudulent credit card application was submitted in Individual 2's name using an email address with the domain name "Ultramilesclub.com." As noted above, law enforcement has obtained evidence indicating that **ADEYEMI** controls that domain name, among others. Victim Bank 1 sent the card associated with this Compromised Account to an address in or around Duluth, Georgia. Notably, Adeyemi Email Account 1 was accessed in March and April 2017 from an IP address that was subscribed to a residence in Duluth, Georgia. Records provided by the United States Postal Inspection Service demonstrate that, in or around April 2018, **ADEYEMI** changed his address to this same address in Duluth. Victim Bank 1 reported that this Compromised Account was used in or around Duluth, Georgia, resulting in approximately \$5,251 in losses to Victim Bank 1.

B. The CW and the Recorded Calls with ADEYEMI

11. Law enforcement has received information from a cooperating witness (the "CW") regarding **ADEYEMI**'s involvement in activity related to credit card fraud. Information provided by the CW has been corroborated by other evidence obtained in the investigation and law enforcement has determined that it is accurate.

12. The CW has engaged in several consensually recorded telephone calls with **ADEYEMI**. The CW contacted **ADEYEMI** using a telephone number that law enforcement has confirmed **ADEYEMI** uses. During the conversations, the CW spoke with **ADEYEMI** about his (the CW's) legal challenges relating to federal criminal charges that the CW is facing in the District of New Jersey in connection with a separate credit card scheme. In these calls, **ADEYEMI** made admissions about his involvement in the scheme, including acknowledging his use of at least one of the Adeyemi Email Accounts. **ADEYEMI** also took various steps in these communications to conceal his identity, including by scolding the CW for referring to him by "AK" in one of the

calls, using an application that disguises voices, and speaking in Yoruba rather than English. Below are excerpts of some of the recorded conversations as translated by a law enforcement translator.

13. On or about June 6, 2018, the CW spoke with **ADEYEMI** in a recorded telephone call. During the call, the CW stated that he had met with his attorney and law enforcement officials in connection with his pending case, and that law enforcement had asked him about other potential co-conspirators. The CW told **ADEYEMI** that law enforcement asked about the name "Alec Dorch," which is an alias **ADEYEMI** has used and is incorporated in part into the email addresses associated with the Adeyemi Email Accounts. The following conversation took place:

CW: He also mentioned some names and asked if I knew anything about them.

ADEYEMI: Okay.

CW: He mentioned one particular name like Alec Dorch or something like that. He asked if I knew who used that name and I told him I don't know.

ADEYEMI: That's crazy.

CW: I don't know how they managed to get that name.

CW: That's why I want to ask you too because I don't know how they got the name.

ADEYEMI: Did they ask for the email that was linked to the name?

CW: Yes, that's what they asked for.

ADEYEMI: Did you speak with the people directly?

CW: I spoke with my lawyer and the prosecutor because I told my lawyer I wanted to talk with them. He asked me why and I told him I did everything they charged me with and how I spent the credit cards.

ADEYEMI: Okay.

CW: They asked me some few questions and promised to get back to me. They showed me some pictures and I told them I've not seen some of those faces before. They also mentioned some names which I told them I don't know the people.

ADEYEMI: I hope my picture is not among the pictures they showed you?

CW: No, your picture is not part of it but your picture is among the general pictures of all the guys in the county.

ADEYEMI: Okay, let's go back to the Alec name again.

CW: Okay.

ADEYEMI: What email is the name linked with?

CW: I don't know if it's Yahoo or Gmail but I will call and ask again.

ADEYEMI: Do you remember if I've used that name before?

CW: Yes, I know you have used it before.

ADEYEMI: This phone I'm using changed my voice right?

CW: Yes it does.

ADEYEMI: Okay, does the email end with 99?

CW: That's possible.

ADEYEMI: I know I've used it before but I can't remember the full details. But I'm positive I've used it before.

CW: Okay.

ADEYEMI: Now, my question is this. Have I ever used it to send stuff to you?

CW: I don't think so because I checked my emails and there is nothing close to that email.

ADEYEMI: Okay.

Based on the context of this and other communications reviewed in the investigation, **ADEYEMI** likely was expressing concern to the CW that law enforcement had inquired about the Adeyemi Email Accounts, and the Alex Dorch alias. Notably, two of the three Adeyemi Email Accounts end in the numbers "99." Further, during this portion of the conversation, **ADEYEMI** checked with the CW to confirm that the application he was using to disguise his voice was working ("This phone I'm using changed my voice right?"). In a follow-up call later the same day, **ADEYEMI** continued to express concern about the email account, stating, "I'm still thinking about the email," "They will be searching for the person that is linked to the email," "Do they show you the full email address?" and "I just want to know more about the email address."

14. In an earlier consensually recorded call on or about May 30, 2018, the CW and **ADEYEMI** also spoke about the CW's interactions with law enforcement and, in particular, various federal criminal prosecutions that have been brought in the District of New Jersey. During the conversation, **ADEYEMI** stated, "Nobody knows what's going on in New Jersey. We have to be careful ... I'm tired. I'm just lying low right now." Later in the call, in discussing the evidence law enforcement may have collected against the CW, the CW stated, "I did not tell anybody you gave me anything," likely referring to Compromised Account information, and **ADEYEMI** stated, "There is no way anybody will be able to connect both of us."

C. JATO's Use of the Compromised Accounts

15. As noted above, **JATO's** role in the scheme included using credit cards associated with the Compromised Accounts at retail stores. Law enforcement has reviewed images from video surveillance footage of transactions involving the Compromised Accounts, including multiple images of an individual matching **JATO's** general appearance. These transactions occurred at retail stores in the Atlanta Georgia area in or around March and April, 2017. Evidence obtained in the investigation revealed that **JATO** has on numerous occasions traveled to that area of Georgia.

16. Specifically, on or about April 8, 2017, a Compromised Account in the name of Victim Cardholder 2 was used at a retail store in or around Lawrenceville, Georgia to make a purchase in the amount of \$397.32. The individual in the surveillance image matches **JATO's** general appearance. Victim Bank 1 has confirmed that the account used for this transaction was a Compromised Account. Victim Bank 1 sustained a loss of approximately \$5,140 in connection with this account.

17. In addition to using Compromised Accounts to make purchases, **JATO** also coordinated with other co-conspirators who retrieved fraudulent credit cards that Victim Bank 1 shipped. For example, on or about January 11, 2017, a co-conspirator not charged as a defendant herein ("CC#4") was arrested by state law enforcement officials near a residence in Bergen County, New Jersey. Prior to his arrest, CC#4 was attempting to retrieve a package from the porch of a residence. Law enforcement subsequently seized a cell phone from CC#4 and obtained a search warrant for it. A review of the cell phone revealed instant messaging communications with a phone that law enforcement has determined **JATO** uses based on subscriber records and toll records, among other things. These communications include instructions that **JATO** provided to CC#4 for picking up the credit card from the residence in Bergen County, including the address of the residence and the name of the cardholder.