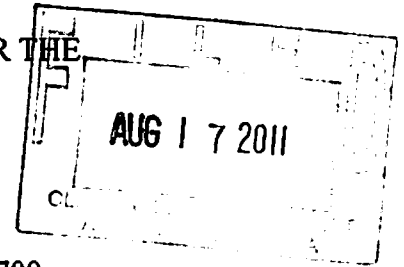


IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division



UNITED STATES OF AMERICA)
)
v.)
)
OLUBUNMI OLADAPO KOMOLAFE,)
aka "DAPSON,")
RAOUL LYCORISH,)
aka "BJ,")
ANTHONY DANERO THOMAS,)
)
Defendants.)

Crim. No. 1:11-MJ-700

UNDER SEAL

**AFFIDAVIT IN SUPPORT OF CRIMINAL COMPLAINT
AND ARREST WARRANTS**

I, Morgan West, Special Agent of the United States Secret Service, being duly sworn,
state:

INTRODUCTION

1. I submit this affidavit in support of a criminal complaint charging OLUBUNMI OLADAPO KOMOLAFE, RAOUL LYCORISH, and ANTHONY DANERO THOMAS with conspiracy to commit access device fraud in violation of 18 USC § 1029(b)(2). I also respectfully request that arrest warrants be issued for KOMOLAFE, LYCORISH, and THOMAS.

2. I have been a Special Agent of the United States Secret Service since 2007. I am currently assigned to the Washington Field Office in Washington, D.C. My duties as a Special Agent include the investigation of counterfeiting and financial fraud. During the course of my law enforcement career, I have investigated multiple cases of financial fraud. In addition, in preparation for my duties as a Special Agent, I received extensive training in the investigation of counterfeiting and financial institution fraud, including training in the investigation and

enforcement of criminal law at the Federal Law Enforcement Training Center. I am authorized to investigate violations of the laws of the United States.

3. I am currently assigned to investigate individuals who illegally use credit card information (access devices) to defraud merchants and financial institutions.

4. The facts and information contained in this affidavit are based upon my training and experience, participation in similar investigations, personal knowledge, interviews of witnesses, as well as the observations of other officials involved in this investigation, including federal, state and local law enforcement officials whom I know to be reliable and trustworthy. All observations not personally made by me were related to me by the individuals who made them or were conveyed to me by my review of records, documents, and other physical evidence obtained during the course of this investigation. This affidavit contains information necessary to support probable cause and is not intended to include each and every fact and matter observed by me or known to the Government.

BACKGROUND

5. Credit card re-encoding is a form of access device fraud, and it begins with stealing a credit card number. Credit card numbers can be stolen in many ways. A common method of stealing credit card numbers is by "skimming," whereby a victim's card is run through a small electronic device that captures the number from the magnetic strip. Skimming can occur during the course of a legitimate transaction, and the victim whose card has been skimmed gets their credit card back (as opposed to having it stolen, by, for example, a pickpocket). Another method of stealing credit card numbers is through electronic means, such as using the Internet to hack into a retailer's computer system and stealing credit card numbers used at the retailer. A common factor in skimming cases and computer hacks is that the victim has possession of their card when its number is being used for unauthorized purchases. Once a credit card number has been stolen

by skimming or computer hacking, it is often re-encoded to a card with a magnetic strip that can function as a credit card. The end result is a card whose number on the front does not match the number encoded on the magnetic strip. A stolen credit card number can be re-encoded many times on many different cards with magnetic stripes, and the stolen number can be used by a suspect until the victim or the victim's servicing financial institution detects the fraud and disables the card number. Suspects sometimes use re-encoded cards to purchase merchandise that is later returned for cash. More frequently, suspects use re-encoded cards to purchase gift cards. The suspects then use the gift cards to purchase merchandise that is later returned for cash. Once a gift card's value is exhausted, it is still useful to a criminal, who can re-encode it with a stolen credit card number. Once the gift card is re-encoded with a stolen credit card number, a suspect can use it to purchase merchandise or more gift cards, and the cycle begins again.

6. KOMOLAFE, LYCORISH, and THOMAS have been associates since at least late 2008. They commit access device fraud and related crimes both together and separately.

7. William Samuel Martin and Usman Muhammad are co-defendants in a credit card fraud case that has been charged in the Eastern District of Virginia.

DETAILS OF THE SCHEME

The Illegally Re-encoded Access Devices

8. On or about January 30, 2010, Martin attempted to make a purchase at Macy's in Arlington, Virginia, using gift cards that had been re-encoded or purchased using a stolen credit card number. Due to his suspicious use of gift cards, a Macy's employee called the Arlington County Police Department ("ACPD"). An ACPD officer located Martin and briefly detained him for questioning. Martin was questioned by the officer inside the security office at the Macy's. Martin consented to a cursory search of his person, and the officer found several gift cards.

Martin voluntarily surrendered the cards to the officer. Martin said that he had obtained the gift cards from his roommate.

9. The ACPD officer who stopped Martin sent Martin on his way because there was nothing obviously fraudulent about the gift cards, and Martin's purchases went through. Later, the officer gave the cards to an ACPD detective, who ran the cards through a Bank Identification Number ("BIN") reader. A BIN reader visually displays the card number on the magnetic strip of a card. When the detective swiped the cards Martin had surrendered to police through the BIN reader, it showed that all of the cards had been re-encoded.

10. I researched the numbers that came up on the BIN reader and found that all of them were issued to victims living outside of Virginia. Many charges were made using the card numbers after Martin voluntarily surrendered his re-encoded cards. The charges include repeated purchases of gift cards at various merchants, many of them within several miles of Martin's residence.

11. I have researched the stolen credit card numbers on the cards that Martin voluntarily surrendered. From approximately January 26, 2010 through approximately February 8, 2010, the fraudulent use of those card numbers caused approximately \$5,875 in fraud loss, plus approximately \$811 in attempted loss to four separate financial institutions.

12. Martin did not surrender all of the cards in his possession to ACPD when he was detained. The receipt for Martin's purchase at Macy's shows that Martin made the purchase using a gift card. Bank and merchant records show that this gift card was purchased on January 16, 2010 in Temple Hills, Maryland using a stolen credit card number. The number on the gift card, however, was not on any of the magnetic strips on any of the cards that Martin voluntarily surrendered. This indicates that Martin had at least one more re-encoded card on his person when he was stopped by the ACPD officer.

13. On June 15, 2010, I interviewed Martin. When asked about the cards Martin surrendered to the ACPD officer on January 30, 2010, Martin stated that he purchased the re-encoded gift cards described above from a person Martin knew only as "Mike." Martin stated that he had just graduated from Bowie State University ("BSU") in Bowie, Maryland and that Mike hangs out on the BSU campus. Martin indicated that many students knew that Mike was dealing in fraudulent credit cards. Martin stated that he purchased the cards from Mike for \$250 each with the understanding that each card had a value of \$500. Martin initially stated that Mike claimed to have received the cards as gifts but later admitted that he knew there was something illegal about the cards.

14. On or about February 18, 2011, LYCORISH, THOMAS, and Martin made several purchases at a Target store in Silver Spring, Maryland. First, THOMAS used a fraudulently re-encoded credit card to buy clothing at a point-of-sale register in the rear of the store. Next, LYCORISH, THOMAS, and Martin went to the front of the store together. There all three of them split up and went to separate registers where each suspect separately used a different fraudulently re-encoded credit card to make purchases totaling approximately \$811.23. After Martin completed his fraudulent purchase with a re-encoded credit card, he noticed that the illegally re-encoded cards THOMAS was trying to use were being declined. Martin immediately went over to THOMAS and swiped the fraudulently re-encoded card he had just used to complete his illegal transaction to complete THOMAS's illegal transaction. The three suspects left the store together and spoke briefly before LYCORISH and THOMAS got into LYCORISH's car to leave. Martin left in a separate car.

15. On or about June 1, 2011, LYCORISH, THOMAS, and Martin again defrauded the Target in Silver Spring, Maryland, by using illegally re-encoded credit cards. First, THOMAS purchased merchandise on a fraudulent re-encoded credit card. Then, THOMAS returned to the

parking lot and got in his own car. Next, LYCORISH purchased merchandise and gift cards using fraudulent re-encoded credit cards. LYCORISH then joined THOMAS in THOMAS's car. Finally, Martin purchased merchandise and a gift card using fraudulent re-encoded credit cards. While Martin was making his illegal purchase, THOMAS brought the car around, and after Martin's purchases were complete, Martin joined THOMAS and LYCORISH in THOMAS's car.

16. On or about August 5, 2011, LYCORISH was arrested by the Montgomery County, Maryland Police Department on an open warrant for credit card fraud. Following his arrest, and after signing a standard waiver of his right to silence and counsel, LYCORISH confessed to participating in a long-running credit card fraud scheme. LYCORISH admitted to recruiting restaurant servers to skim credit cards, using re-encoded cards, and making purchases designed to conceal the source of his illegally derived funds. LYCORISH admitted that he had made such purchases at the Nordstrom in Tyson's Corner, Virginia, within the Eastern District of Virginia.

Going on "Moves"

17. On or about February 22, 2011, law enforcement conducted surveillance as Muhammad led a criminal scheme where gift cards were purchased with forged access devices, and merchandise purchased with fraudulently obtained gift cards was returned for cash.

18. Confidential Informant 1 ("CI1") is an associate of Muhammad's. I know CI1 to be credible from their track record, the fact that they have made statements against their own interest, and my corroboration of CI1's statements. "Moves" is a term Muhammad and others use to collectively refer to the purchasing of gift cards with forged access devices and the return of merchandise purchased with fraudulently obtained gift cards. CI1 has worked as a "runner" for Muhammad many times. Runners help criminals conceal their activity. Runners fill many roles in credit card fraud cases. Some runners will be given a forged access device and directed to buy gift cards. Other runners will be directed to purchase merchandise with the gift cards. Still other

runners will be given the fraudulently obtained merchandise and directed to return it to a retailer for cash. Nordstrom is particularly favored by criminals committing access device fraud because Nordstrom has a lenient return policy and will accept returns and give the customer cash. CII's return history at Nordstrom totals approximately \$24,774 and is mostly confined to returns made at stores in Fairfax County and Arlington, Virginia, within the Eastern District of Virginia.

19. On or about February 21, 2011, Muhammad called CII and asked that CII go on "moves." Muhammad also told CII that CII would be returning a pair of expensive shoes to a Nordstrom store.

20. On or about February 22, 2011, law enforcement observed Muhammad pick CII up at CII's residence. Muhammad was driving a vehicle registered to KOMOLAFE, who was also in the car. CII had an audio recording device on their person. Muhammad drove CII and KOMOLAFE to a Target store in Bowie, Maryland. This particular Target store's own receipts, however, show it in Lanham, Maryland.

21. CII told me that when they arrived at the Target, Muhammad gave CII several gift cards, which CII understood had been re-encoded with stolen credit card numbers. CII entered the Target store and used the cards Muhammad had provided to purchase approximately \$2,500 of gift cards. While CII was inside the Target making the purchases, KOMOLAFE was also inside, watching CII and conducting counter-surveillance. When CII returned to the car, CII gave the gift cards to Muhammad.

22. Next, Muhammad drove CII and KOMOLAFE to a Target store in Wheaton, Maryland. Along the way, KOMOLAFE made comments to Muhammad about how relaxed CII seemed.

23. When the car arrived at the Wheaton Target store, CII observed Muhammad operate a laptop computer. CII told me later that they watched Muhammad type a few keystrokes

into a program, and then a name would appear with a long string of numbers. Muhammad would delete the name, and then swipe a credit card through a piece of electronic hardware attached to the computer. CI1 said that this was Muhammad's process to re-encode cards. CI1 said that Muhammad would delete the name from the screen because that prevented the name from being printed on any receipts. A printed name on a receipt might arouse the suspicions of a store clerk if the name did not appear to match the customer making the purchase (e.g., a woman's name and a male customer). I know from training and experience that CI1's description of Muhammad's swiping of cards is an accurate description of the process by which access devices are re-encoded with stolen credit card numbers.

24. After Muhammad illegally re-encoded several access devices, he gave the forged access devices to CI1. The re-encoded access devices were to be used for purchasing gift cards.

25. Law enforcement watched as all three people exited KOMOLAFE's car. Muhammad put an object in the trunk of the car, which CI1 told me later was the electronic device that Muhammad was using to re-encode cards.

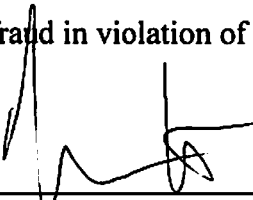
26. Law enforcement watched all three people as they entered the Wheaton Target store. Inside, CI1 purchased approximately \$1,750 of gift cards. When CI1 returned to the car, CI1 gave the gift cards to Muhammad.

27. I arrested Muhammad on July 14, 2011. In interviews following his arrest, Muhammad confessed to using illegally re-encoded access devices. Furthermore, I seized a computer from the car Muhammad was driving when he was arrested. I obtained a search warrant for the car and computer, signed by the Honorable Theresa C. Buchanan. A forensic exam of the computer is ongoing, but preliminary results show that the computer contains numerous stolen credit card numbers, and that the computer had been accessed by several different users. Muhammad told me that to the best of his recollection the stolen credit card numbers he was

fraudulently re-encoding on February 22, 2011 were obtained by KOMOLAFE. Muhammad also said that KOMOLAFE is currently in possession of the piece of computer hardware that is used to actually re-encode credit cards.

CONCLUSION


28. Based on the information contained in this affidavit, there is probable cause to believe that in or about January 2010, through June 2011, in the Eastern District of Virginia and elsewhere, OLUBUNMI OLADAPO KOMOLAFE, RAOUL LYCORISH, and ANTHONY DANERO THOMAS, conspired with William Samuel Martin and Usman Muhammad, who have already been charged, to commit access device fraud in violation of 18 U.S.C. § 1029(b)(2).



Morgan West
Special Agent
United States Secret Service

Approved by: SAUSA Andrew K. Mann

Sworn to and subscribed before me
this 17th day of August, 2011,
/s/



Theresa Carroll Buchanan
United States Magistrate Judge
Hon. Theresa C. Buchanan
United States Magistrate Judge
Alexandria, Virginia