ORIGINAL FILED

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

NOV 2 0 2008

CLAIRE C. CECCHI, U.S.M.J.

UNITED STATES OF AMERICA	:	
	:	**CRIMINAL COMPLAINT**
-v-	:	
	:	Mag. No. 08-4163
DERRICK POLK	:	
	:	Hon. Claire C. Cecchi

I, Scott Marino, being duly sworn, state the following is true and correct to the best of my knowledge and belief. Between in or about December 2007 and in or about July 2008, in the District of New Jersey and elsewhere, defendant Derrick Polk did:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.

Scott Marino

Scott Marino, Special Agent
Federal Bureau of Investigation

Sworn to before me and subscribed in my presence,
November 20, 2008, in Essex County, New Jersey

Claire C. Cecchi

HONORABLE CLAIRE C. CECCHI
UNITED STATES MAGISTRATE JUDGE

Signature of Judicial Officer

ATTACHMENT A

COUNT I

Between in or about December 2007 and in or about July 2008, in the District of New Jersey and elsewhere, defendant

DERRICK POLK

did knowingly and intentionally conspire with O.A., O.O., J.O., and O.C. and others to transfer, possess and use means of identification of other persons without lawful authority, in a manner affecting interstate commerce, with the intent to commit, and in connection with, unlawful activity constituting a violation of federal law, namely, 18 U.S.C. § 1343, contrary to 18 U.S.C. § 1028(a)(7) and (b)(1).

In violation of Title 18, United States Code, Section 1028(f).

COUNT II

Between in or about December 2007 and in or about July 2008, in the District of New Jersey and elsewhere, defendant

DERRICK POLK

did knowingly and intentionally conspire with O.A., O.O., J.O., and O.C. and others to devise a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing such scheme and artifice, did transmit and cause to be transmitted by means of wire communications in interstate commerce, certain writings, signs, signals, and sounds, as described below, contrary to Title 18, United States Code, Section 1343.

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

COUNT III

Between in or about December 2007 and in or about July 2008, in the District of New Jersey and elsewhere, defendant

DERRICK POLK

did knowingly and willfully conspire and agree with Hakeem Olokodana, O.A., O.O., J.O., O.C., and other persons to commit crimes against the United States, that is, to knowingly and with intent to defraud, access protected computers without authorization, and exceed authorized access and by means of such conduct to further the intended fraud and obtain things of value, contrary to Title 18, United States Code, Section 1030(a)(4).

OVERT ACTS

In furtherance of the conspiracy and to effect its unlawful object, the following overt acts were committed in the District of New Jersey and elsewhere:

a. On or about May 14, 2008, Hakeem Olokodana accessed the Bank of America bank account of a third party without authorization.

b. On or about May 15, 2008, Hakeem Olokodana accessed the Washington Mutual bank account of a third party without authorization and changed the mailing address on the account.

In violation of Title 18, United States Code, Section 371.

ATTACHMENT B

I, Scott Marino, a Special Agent of the Federal Bureau of Investigation, have knowledge of the following facts based upon evidence collection during the investigation, discussions with witnesses and other law enforcement agents. Since this affidavit is submitted for the purpose of establishing probable cause to support the issuance of a complaint and arrest warrant, I have not included each and every fact known by the government concerning this investigation. Statements attributed to individuals are provided in substance and in part.

Between on or about May 8, 2008 and on or about July 24, 2008, the FBI intercepted wire communications pursuant to court orders. Descriptions of calls below are based on summaries of the conversations.

SUMMARY OF THE INVESTIGATION

1. Beginning in or about November 2007, the FBI and other law enforcement agencies have been investigating a multi-national identity theft ring. That organization, which operates in the United States, the United Kingdom, Canada, China, Japan, Vietnam, and South Korea, among other places, is involved in acquiring identity information and using that information to conduct numerous fraudulent schemes, with an emphasis on frauds relating to depleting their victims' home equity line of credit (HELOC) accounts, as well as other schemes to withdraw funds from bank and credit accounts.

2. The perpetrators initiate the fraud by gaining access to confidential customer and account information used by customers of banks, credit unions, and credit card issuers to conduct financial transactions in the United States. This information includes account holder names, addresses, dates of birth, account numbers, Social Security numbers, and account balances. Other account information frequently obtained by the coconspirators during the course of the fraud includes mothers' maiden names, security question answers, on-line user names, passwords, and other data used by banks and lending institutions to service and secure customer accounts.

3. The investigation to date has revealed that customer account information relating to several large and small banks, credit unions, and credit issuers throughout the United States has been compromised. The larger institutional victims to date include Citibank, JPMorganChase, Wachovia, Washington Mutual, and Bank of America, among others. Dozens of smaller banks and credit unions have also been victimized, including the Navy Federal Credit Union, Pentagon Federal Credit Union, U.S. Senate Federal Credit Union, the State Department Federal Credit Union, and at least approximately eleven New Jersey-based financial institutions.

4. The investigation to date has revealed that one prong of the identity theft ring involves the withdrawal of funds from HELOCs belonging to innocent customers of banks and credit unions. Confirmed losses to date relating to the HELOC scheme alone exceed $2.5 million, with at least approximately $4 million more in attempted but ultimately

unsuccessful transfers. The victims, among others, include two account holders at Affinity Federal Credit Union of Basking Ridge, New Jersey ("Affinity"), two account holders at Financial Resources Federal Credit Union of Bridgewater, New Jersey ("FRFCU"), at least one account holder at San Francisco, California-based First Republic Bank, and one account holder at First Financial Federal Credit Union of Toms River, New Jersey. For example, on or about April 29, 2008, the co-conspirators attempted to victimize Grand Bank & Trust of West Palm Beach, Florida in the approximate amount of $317,000, and First Citrus Bank of Tampa, Florida in the approximate amount of $266,000. Likewise, on or about July 16, 2008, the co-conspirators attempted to victimize Florida-based Vision Bank in the approximate amount of $125,000.

5. As part of the scheme, the coconspirators obtain account and personal identifying information belonging to HELOC account holders at various banks and credit unions. Based on e-mail accounts searched in connection with the investigation to date, as discussed below, the coconspirators obtain at least some of this identifying information via e-mail from coconspirators with domestic and foreign-based e-mail addresses. The co-conspirators also mine public filings and records (including property deeds and mortgages) and publicly available Internet databases to obtain credit applications, credit reports, and signature exemplars.

6. Based on interviews with banks that have been victimized and Court-authorized monitoring of a cellular telephone facility connected to the fraud, the coconspirators expand on that account and personal identifying information through social engineering. That is, the coconspirators place telephone calls to banks and credit unions at which HELOC accounts are maintained and, through interaction with unwitting customer service representatives and loan officers, extract additional customer and account information by posing as legitimate account holders.

7. With sufficient customer information on hand, the co-conspirators contact the banks and credit unions, again posing as the legitimate account holder. The co-conspirators use prepaid calling cards, dial *67, and employ other technologies to block caller ID in an effort to hide their own identity and further the fraud. During the call with a bank, or by facsimile, the co-conspirators request that a large percentage of the balance of a victim HELOC be wired to a pre-selected bank account controlled by the coconspirators. When the wire request is done by facsimile, the victim account holder's signature is copied from publicly filed documents available as part of mortgage and HELOC records to verify a lien on a house.

8. Banks and credit unions typically verify the authenticity of a wire request by contacting their customer at a telephone number that is already on file with the bank. To circumvent this security protocol, the co-conspirators use one of two techniques to "re-route" the verification call. One technique involves persuading bank officials to change the account holder's telephone number on file to a number chosen by the co-conspirators, thereby ensuring

co-conspirators contacting the account holder's local telephone company (e.g., Verizon) to report a fake technical problem, and thereby persuade the local telephone company to forward all of the customer's inbound telephone calls to a telephone number pre-selected by the co-conspirators.

The co-conspirators then "authenticate" the wire request by impersonating the account holder during the bank's verification call. HELOC funds are then wired in accordance with the co-conspirators' fraudulent instructions.

9. By the time either the victim bank or victim HELOC customer discovers the unauthorized transfers – after requesting an account balance or receiving an account or transaction statement – the co-conspirators have drained a significant percentage of the HELOC's available credit. Stolen funds have subsequently been transferred to coconspirators in Japan, Nigeria, South Korea, and Canada, among other countries.

10. As an alternative to requesting wire transfers out of the victim HELOC accounts, the coconspirators gain online access to the HELOC accounts by setting up online accounts in the victim's names at the banks or by acquiring the usernames and passwords of the account holders. To avoid detection, the co-conspirators routinely access the Internet using wireless Aircards acquired in either false names or the names of identity theft victims or by using open wireless (Wi-Fi) signals registered to unwitting third parties. After establishing the online accounts, the co-conspirators deplete the accounts by transferring funds to other accounts and withdrawing the funds from all the accounts.

11. In connection with the scheme, the perpetrators also direct the victim banks, credit unions and card issuers to change customer addresses on file to addresses controlled by the coconspirators ("Drop Addresses"). In this way, the coconspirators are able to prevent statements and confirmations that would otherwise alert account holders to unauthorized transfers from being sent to the victim account holders. Similarly, the perpetrators use the Drop Addresses to receive checks, or replacement debit and credit cards, that can be used to further drain victim customers' accounts.

THE G.K. TRANSACTION

12. On or about December 17, 2007, Hakeem Olokodana, a coconspirator who is not charged as a defendant herein ("Olokodana"), contacted Affinity by telephone purporting to be an Affinity HELOC customer bearing the initials G.K. ("G.K."). At the time, G.K. had access to an approximately $800,000 HELOC with a zero balance. Posing as G.K., Olokodana requested a $675,600 wire transfer drawn on G.K.'s Affinity HELOC and directed that the funds be wired to an account at Bank of Tokyo Mitsubishi in the name of Mosdaf Investments. The Affinity representative, who did not realize that he was dealing with Olokodana and not G.K., followed the bank's security protocols by quizzing Olokodana regarding G.K.'s identifying information. Olokodana knew G.K.'s identifying information and successfully answered all of the security questions.

two hours after the original call, in an attempt to authenticate the $675,000 wire request, an Affinity representative called G.K. at the telephone number in Affinity's file. The Affinity representative's phone call was answered, and the call recipient identified himself as G.K. In

reality, the Affinity representative was unknowingly speaking with Olokodana, who had made the initial wire request. Olokodana confirmed the wire request to the Bank of Tokyo Mitsubishi and answered additional security questions that the Affinity representative asked. Thereafter, the wire instructions were executed and G.K.'s HELOC balance went from zero up to approximately $675,600.

14. On or about December 18, 2007, a coconspirator in Japan withdrew approximately $675,600 from the Mosdaff Investments Bank of Tokyo Mitsubishi account.

Getting Around Affinity's Verification Call

15. Records received from Verizon reveal that on or about December 17, 2007, G.K's home telephone service provider was Verizon. Verizon was contacted on or about December 17, 2007, purportedly by G.K. During that call, the person identifying himself as G.K. represented to Verizon that a problem existed with the telephone and asked that all incoming calls be forwarded to (646) 200-5790.

16. On or about December 17, 2007, the number (646) 200-5790 was associated with an Internet-based call forwarding service known as Kallback ("the (646) 200-5790 Kallback Number"). Accounts maintained at Kallback can be configured to forward incoming calls to a previously determined number ("Ring-To Number").

17. Records received from Kallback indicate that on or about November 6, 2007, an individual, later identified as Olokodana, contacted Kallback, claimed to be "Shawn Anderson," and opened an account ("the Shawn Anderson Kallback Account"). The (646) 200-5790 Kallback Number, among others, was used with the Shawn Anderson Kallback Account.

18. Kallback's records reveal that all incoming calls to the (646) 200-5790 Kallback Number, including Affinity's December 17, 2007 call to verify G.K.'s wire request, were forwarded to an AT&T Wireless cellular telephone number (480) 543-9837 ("the 9837 Ring-To Number") which was used by Olokodana. Call records reveal that other incoming calls to the (646) 200-5790 Kallback Number that were forwarded to the 9837 Ring-To Number also originated at banks and credit unions.

19. Kallback records reveal that between on or about November 7, 2007 and on or about January 18, 2008, "Shawn Anderson" set up six additional Kallback Numbers programmed to forward telephone calls to the 9837 Ring-To Number. During that same period, approximately ten calls to those additional Kallback Numbers also originated from banks and credit unions, including calls from FRFCU and First Financial Federal Credit Union on the days that those credit unions were victimized.

20. Kallback records revealed that to register for Kallback accounts, Olokodana used Yahoo e-mail accounts, including the e-mail account kuhndert527@yahoo.com (the "Kuhndert E-Mail Account").

THE J.C. TRANSACTION

21. On or about March 12, 2008, First Florida Bank, a bank operating in Florida, received a telephone call from an individual purporting to be First Florida customer "J.C.", who requested a change in the home telephone number affiliated with the account. The caller answered security questions and was able to change the telephone number associated with the account to 239-348-5253 (the "5253 Number").

22. On or about April 2, 2008, First Florida received a fax, purportedly from J.C., that included a request for a wire transfer in the amount of $248,645 from J.C.'s HELOC account to the account of Pembroke Title Co. at TFC Bank in Chicago. To verify the wire request, a First Florida representative called J.C.'s "new" phone number – the 5253 Number – to verify the request. The person answering the phone confirmed the wire request and answered security questions. Later that day, First Florida wired the money to the TCF Bank account of Pembroke Title Co. During transmittal of the wire, First Florida received a telephone call from an individual purporting to be J.C. wanting to confirm that the wire had been sent. The caller ID at the bank showed the caller's phone number as the 5253 Number in the name of Bello Salako, an alias used by Olokodana.

23. On or about April 16, 2008, the real J.C. contacted First Florida and advised that he received an account statement showing a balance of $248,660 on his HELOC, however, he advised that he had not conducted any transactions on the account.

24. On or about April 18, 2008, an individual claiming to be J.C. called First Florida to inquire about the balance of his HELOC account. The caller ID at the bank indicated that the call was coming from a number that the investigation tied back to a phone registered to Bello Salako but used by Olokodana. In addition to trying to avoid detection by registering the phone in Salako's name, Olokodana further tried to avoid detection by placing calls using a calling card and also dialing *67, which has the effect of blocking caller ID information.

25. The FBI has received records from TCF Bank which indicate that almost all of money wired into the Pembroke Title account from the J.C. account was withdrawn through a series of account transfers, ATM withdrawals, and cashier's checks within fifteen days of the April 2, 2008 wire.

USE OF E-MAILS TO TRANSFER IDENTITY INFORMATION

26. Court-authorized searches of over twenty e-mail accounts reveal that e-mail was used extensively by co-conspirators to facilitate the transfer of stolen identity information,

27. On or about April 25, 2008, the FBI searched the Kuhndert E-Mail Account, which contained approximately 133 e-mails. These e-mails contained wire authorization

requests from banks and credit unions around the United States; personal and account information for bank and credit union customers from New Jersey, Florida, and elsewhere; and evidence suggesting that such data is either gathered using publicly available electronic databases or delivered via e-mail as a complete package of identifying information.

28. Between December 6, 2007 and January 14, 2008, the Kuhndert E-Mail Account received wire authorization forms from, among other institutions, BMS Federal Credit; Union; FDU Federal Credit Union; L'Oreal USA Federal Credit Union; First Constitution Bank; New Jersey Gateway Federal Credit Union; North Jersey Federal Credit Union; Novartis Federal Credit Union; Picatinny Federal Credit Union; Self Reliance Federal Credit Union; and United Teletech Financial.

29. On or about October 12, 2007, Olokodana, using the Kuhndert E-Mail Account, received an e-mail from a coconspirator in the United Kingdom. The e-mail contained the following information[1]:

> 1st name: cxxxxxxx
> last name: wxxxxxxx
> ss#:148-46-xxxx
> dob:06-1x-x1
> mmn: mxxxick
> addr:5 xxxxxx xxxx rd
> xxxxx xxxxx, nj. 0xxx1
> hm#:7xx530xxxx
> ise: first atlantic fed credit union
> line avail: 5xx,xx0
> bal owe : 27,835
> member acct: unknown (he has a lot of money in is [sic] account)
> union addr: 4xx inxxxxxxl way west
> xxxx town,nj 07724
>
> ill give you a call bye.

30. On or about April 25, 2008, a coconspirator in Canada identified herein as "Charlie" received an e-mail containing the following information:

> ONLINE ID- xxxxxing08
> PASSWORD-pexxxx22
> necessary answers to questions
> 1-ackah

---

[1]All personally identifiable information and account information has been redacted.

3-london
routine no-05xxxx483
account no-22xxxxxxxx73

bank address
bank of america,SC3-198-01-01
104 Regency Drive
Columbia SC 29212
PH-803-726-1376

31. A court-authorized search of Charlie's e-mail account revealed that between in or about July 2007 and in or about April 2008, that individual exchanged at least approximately 40 e-mails with defendant POLK, including e-mails in which he passed on requests from Olokodana for account information relating to third parties.

32. On or about April 3, 2008, defendant POLK, who was using the e-mail account derrickpolk@ca.rr.com (the "Derrick Polk E-Mail Account"), sent an e-mail to Charlie. In the e-mail, defendant POLK transferred Charlie the following stolen account information:

Gxxxxx Financial Services
Comerica Bank
One North Central Ave Ste 110
Phoenix, AZ 85004
Personal Ac XXXX99729
Rtn XXXX7522
Buisness Ac XXXXX2160

I have not as the time of this mail received Pin for online. Will send as soon as gotten.

33. On or about April 3, 2008, defendant POLK sent a second e-mail to Charlie containing stolen identity information for a third party, including the name, address, American Express number, customer security number (CVV), and expiration date.

34. On or about May 8, 2008, O.C. used the e-mail account akurre96@yahoo.com to send a list containing the names and addresses of 39 identity theft victims from Arizona, California, Florida, Georgia, Illinois, Indiana, Minnesota, New Jersey, New York, Oregon, Pennsylvania, Texas, and Washington to an e-mail address controlled by Olokodana.

35. On or about May 9, 2008, Olokodana forwarded the list of 39 names to an e-mail

36. On or about May 10, 2008, at approximately 12:42 p.m. (EDT), Y.J. telephoned Olokodana and discussed the list of 39 names in a call intercepted by law enforcement personnel.

Olokodana and Y.J. discussed that "Kunle" -- an alias for O.C. – had sent the 39 names and that the names were all good. Y.J. told Olokodana that all of the names were "good," and that "Kunle" had done "a good job" in verifying the addresses. Y.J. stated further that using those addresses never gave him a problem.

GAINING UNAUTHORIZED ACCESS TO BANK ACCOUNTS

37. Pursuant to court-authorized interception of telephone calls, the FBI has learned that on or about May 14, 2008, at approximately 1:49 p.m., Olokodana and a co-conspirator ("CC1") discussed online access to a Bank of America Account. Olokodana told CC1 that he had just gotten off the phone with Bank of America. Olokodana further indicated that during the conversation he obtained log-in information for a Bank of America customer. Records recovered regarding Olokodana's Internet usage confirm that on or about May 14, 2008 at approximately the same time as this conversation was taking place, Olokodana was navigating his web browser to the IP address 171.159.194.233. A whois lookup reveals that this IP address is registered to Bank of America.

38. Pursuant to court-authorized interception of telephone calls, the FBI has learned that on or about May 15, 2008 at approximately 11:26 a.m., Olokodana and a co-conspirator discussed access to a third party's Washington Mutual bank account. The conversation lasted approximately one hour. During the conversation, Olokodana indicated that he was looking at a bank customer's personal account online. He further indicated that he had successfully changed the customer's billing address. Later in the conversation, Olokodana indicated that he was accessing another Washington Mutual account, this one with a line of credit that was up to $115,900. Records recovered regarding Olokodana's Internet usage confirm that on or about May 15, 2008, at approximately the same time as this conversation was taking place, Olokodana navigated his web browser to the IP address 167.88.184.52. A whois lookup reveals that this IP address is registered to Washington Mutual, Inc.

AVOIDING DETECTION: USE OF WIRELESS CARDS & Wi-FI

39. Records received from Yahoo! reveal that a number of the accounts passing stolen identity information among the coconspirators, including Olokodana's accounts, were accessed from wireless Internet cards, specifically Sprint wireless Aircards. Sprint Aircards provide high-speed Internet access wherever a cell phone can be used.

40. Between on or about February 28, 2008 and April 8, 2008, Olokodana's Kuhndert E-Mail Account was accessed 36 times, all through IP addresses controlled by Sprint. For example, on or about March 4, 2008 at 15:53 (GMT), the Kuhndert E-Mail Account was accessed from IP address 68.245.187.13; on or about March 26, 2005 at 22:20 (GMT), the

2008 at 22:58 (GMT), the Kuhndert E-Mail Account was accessed from IP address 68.245.56.237. Whois lookups reveal that each of these IP addresses is registered to Sprint, and Sprint records revealed that these particular IP addresses were assigned to Shola Bello, an alias

used by Olokodana in furtherance of the conspiracy and to avoid detection.

41. In addition to using Sprint Aircards to avoid detection, members of the conspiracy also used unsecured Wi-Fi signals to access e-mail accounts which were used to pass stolen identity information. For example, on or about June 26, 2008 at 13:45:57 (GMT), July 1, 2008 at 18:27:24 (GMT), and July 3, 2008 at 15:24:37 (GMT), D.Y., a coconspirator who is not charged as a defendant herein, resided in a high-rise luxury condominium building in New York City. At those times and dates, D.Y. used the Wi-Fi access point of another individual in the building to access a Yahoo! e-mail account he used to transmit stolen identity information to Olokodana. On or about June 26, 2008 at 18:01:57 (GMT), D.Y. used the Wi-Fi access point of the luxury condominium's lounge to access the same Yahoo! e-mail account.

DEPLETING HELOC ACCOUNTS BY DIVERTING CHECKS

42. In or about May 2008, Olokodana and his coconspirators were heard on intercepted calls discussing problems with wiring funds out of HELOC accounts due to improved bank security measures. Instead of wiring the money out of the accounts, the co-conspirators sought to change addresses on victim accounts and to ask the banks to deliver new checks, debit cards, and statements to Drop Addresses. The following intercepted conversations between Olokodana and O.O. revealed that O.O. was a supplier of Drop Addresses that Olokodana provided to banks when posing as an account holder:

a. On or about May 13, 2008, at approximately 4:15 p.m., Olokodana called O.O.. O.O. asked Olokodana if he could receive a text message with an address that's "good to go." Olokodana stated that he "hoped the place is OK," to which O.O. replied that the address belonged to a friend of his who was no longer there.

b. On or about May 14, 2008, at 3:55 p.m., Olokodana received an incoming telephone call from telephone number (217) 638-1213, a phone used by O.O.. O.O., who was identified as "Jide", stated that he sent information and an address to Olokodana. Olokodana asked whether the address was "safe." O.O. responded that the address was vacant and normally for rent. O.O. further stated that he uses four "deals" per address. Olokodana asked how long he could use the address because he needed it for 45 days to execute his deal. O.O. stated that 45 days would be fine, but that he normally used addresses for only 30 days. O.O. requested that Olokodana send "those names" so that he could perform his own part of the job.

c. On or about May 15, 2008, at 12:35 p.m., O.O. called Olokodana. Olokodana confirmed with O.O. that he had received information from O.O. and planned to

address was 1904 South Wirt Avenue ("the South Wirt Avenue Drop Address"), and the area code for the neighborhood was (217). O.O. confirmed this information for Olokodana.

d. On or about May 18, 2008, at approximately 7:46 p.m., O.O. called Olokodana. Olokodana told O.O. that he was already using addresses provided by O.O.

e. Between on or about May 15, 2008 and in or about July 2008, Olokodana contacted banks and impersonated customers in furtherance of the conspiracy, in part by giving the South Wirt Avenue Drop Address as a false customer mailing address. For example, on or about June 16, 2008, at approximately 10:40 a.m., Olokodana called Washington Mutual Bank Consumer Loan Services in reference to two different bank accounts. Each time, Olokodana identified himself as a bank customer and provided a mailing address for the bank to send account documents. During the second call, Olokodana requested confirmation of the account address, and was told by a Washington Mutual customer service representative that the account address was the South Wirt Avenue Drop Address.

f. Similarly, on or about June 5, 2008, Hakeem Olokodana called Federal Trust Bank and impersonated "R.W.", a bank customer. Olokodana requested that R.W.'s account address be changed to the South Wirt Avenue Drop Address.

USING THE PHONES AS PART OF THE CONSPIRACY

43. Between on or about May 8, 2008 and on or about June 6, 2008, the FBI intercepted wire communications occurring over a phone used by Olokodana. As set forth by example below, intercepted communications over the phone provided evidence of the involvement of the following coconspirators:

O.A.

a. On or about May 18, 2008, Olokodana received a call from O.A., who identified himself as "Jeff." O.A. left a voicemail requesting a return call. At or about 7:04 p.m., Olokodana returned O.A.'s call. Olokodana asked O.A. whether O.A. had been able to confirm those "things." O.A. stated that he checked all of the customers, but most had drawn upon their entire lines of credit and only three customers had available balances. O.A. further stated that one customer had a $66,000 balance against a $110,000 line of credit, and that another had a zero balance on a $139,000 line of credit. O.A. and Olokodana discussed Bank of America lines of credit, and each stated that he had changed customer addresses in furtherance of fraud. Olokodana stated that he had done "log-in" with some of the customer information he had. Olokodana stated that he did not like deals with small accounts.

b. On or about May 19, 2008, at 5:04 p.m., Olokodana called O.A.. Olokodana stated that he had done "log-ins" into accounts of unsuspecting bank customers. Olokodana asked O.A. if he could begin the transfer because Olokodana had

verified these individuals' account balances. O.A. said yes and provided Olokodana with a destination account for the funds. While Olokodana was on the phone, he indicated he that had been able to add the destination account at Charles Schwab to the customer's (on-line) account. Olokodana and O.A. discussed making two test deposits into the Charles Schwab account for verification. O.A. agreed to notify Olokodana after the request for verification was made. The intended withdrawal was $40,000. In a follow up call at or about 3:19 p.m., Olokodana confirmed to O.A. that he had made the requested transfer.

c. On or about May 23, 2008, at 11:52 a.m., Olokodana called O.A.. Olokodana told O.A. that he had some accounts whose customers had not used their checking accounts for a long time. He planned to transfer money to those accounts, and then move money from the checking account to external accounts gradually. Olokodana stated he planned to do 10 accounts per day in amounts of at least $10,000 per account, which would result in $100,000 in proceeds. Olokodana believed he would be "fine" if he could do that.

J.O.

d. On or about May 14, 2008, Olokodana contacted J.O.. During the course of the conversation, J.O. and Olokodana discussed a $20,000 "deal".

e. On or about May 15, 2008, at approximately 8:39 a.m., Olokodana placed an outgoing call to J.O.. Olokodana asked J.O. whether he had sent money, to which J.O. replied that the money had been sent "pay without ID" (a Western Union Moneygram transmission method) under J.O.'s telephone number. In a follow up call approximately 10 minutes later, Olokadana and J.O. discussed the fact that Western Union had not released the payment to Olokodana. Olokodana stated that he was making money in the United States through identity theft. J.O. stated that he too tried to commit identity theft, but he had not been successful, to which Olokodana replied that if J.O. could get a Bank of America card, money could be made. J.O. stated he was only able to make $1,000 to $1,500 at a time from Bank of America cards. Olokodana stated that he could get more, exhausting $20,000 of a line of credit by "cashing $4,900 repeatedly." In subsequent calls, J.O. indicated that he had completed a Western Union transaction. Olokodana stated he still could not claim the expected Western Union money. The transaction amount was $200. Later, J.O. indicated that he had resent the money through Western Union. Olokodana indicated he would go and collect the money right away.

f. As previously described in paragraph 36, on or about May 10, 2008, at approximately 12:42 p.m. (EDT), Y.J. telephoned Olokodana and discussed the

list of 39 names. Olokodana and Y.J. discussed that "Kunle" had sent the 39 names and that the names were all good. Y.J. told Olokodana that all of the names were good, and that "Kunle" had done a good job in verifying the addresses. Y.J. stated further that using those addresses never gave him a problem.

g. On or about May 15, 2008, Olokodana received a call from O.C. Olokodana indicated that O.C. was involved in identity theft involving Bank of America. Olokodana stated that he planned to do certain "deals" in the first week in June and expected to make $300,000. Olokodana further stated that he has done a lot of computer log-ins involving Washington Mutual cards from his home.

h. On or about May 17, 2008, at 8:38 p.m., Olokodana called O.C., who indicated that he maintained an office in which he did similar work to that done by Olokodana. Olokodana said he was frustrated at how cautious banks were being with lines of credit, including that some institutions were requesting that callers state the purpose of the withdrawal. Olokodana further stated to O.C. the stress that both of them have been going through when it came to getting business done with banks in general and that business has been slow for them.

i. A search conducted on or about August 4, 2008 of Olokodana's "office" revealed that Olokodana maintained over ten cellular telephones, a scanner, blank credit cards, and documents in the names of identity theft victims at the location from which he often made calls to coconspirators.