

SBK/2009R00542

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA
v.

Hon. (WJM)

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"

Criminal No. 11-299

a/k/a "Kris,"

18 U.S.C. § 1343

a/k/a "Steven Bing,"

18 U.S.C. § 1349

CHARLES UMEH CHIDI,

18 U.S.C. § 1028(f)

a/k/a "Charlie,"

18 U.S.C. § 1028A(a)(1)

WAYA NWAKI,

18 U.S.C. § 1030(a)(4)

a/k/a "Jonh Done,"

18 U.S.C. § 1030(b)

a/k/a "Prince Abuja,"

18 U.S.C. § 2

a/k/a "Shawn Conley,"

a/k/a "USAPrince12k,"

OSARHIEME UYI OBAYGBONA,

a/k/a "Uyi Obaygbona,"

a/k/a "bside bside,"

MARVIN DION HILL,

a/k/a "Da Boss,"

a/k/a "Nyhiar Da Boss,"

a/k/a "Nihiar Springs,"

ALPHONSUS OSUALA,

a/k/a "Andrew Johnson,"

a/k/a "jamal j," and

OLANIYI JONES,

a/k/a "Brenda Stuart,"

a/k/a "Olaniyi Victor Makinde,"

a/k/a "Makinde Olaniyi Victor"

INDICTMENT

The Grand Jury in and for the District of New Jersey,
sitting at Newark, charges:

COUNT 1

18 U.S.C. § 1349

(Conspiracy to Commit Wire Fraud)
(All Defendants)

BACKGROUND

I HEREBY CERTIFY that the above and foregoing is a true and correct copy of the original on file in my office.

ATTEST

WILLIAM T. WALSH, Clerk
United States District Court
District of New Jersey

By: [Signature]
Deputy Clerk

1. Between in or about August 2009 and in or about June

2010, the seven defendants named in this Indictment worked together across three continents in an effort to steal millions of dollars. To do so, the defendants used Internet "phishing" attacks and bogus websites to trick unwitting consumers into giving up their online usernames and passwords.

2. Armed with these credentials, defendants added fake employees to the payroll accounts of victim companies at payroll processing companies. They used these victims' online accounts to "pay" the fake employees through electronic transfers. Defendants then divided up the proceeds by transferring them to accounts that they controlled and by wiring money overseas via bank wire, Western Union, and Moneygram.

3. Defendants also used the stolen credentials to access customers' online bank accounts, to gather personal information about their victims, and to make fraudulent withdrawals from the victims' bank accounts. Defendants again divided the proceeds and wired funds overseas.

4. At various times relevant to this Indictment:

Defendants

a. Defendant KARLIS KARKLINS, a/k/a "Susanne O'Neill," a/k/a "Kris," a/k/a "Steven Bing," resided in or near Riga, Latvia. Defendant KARKLINS used the e-mail account susanneon@[Provider 1].com ("the Susan Neon Account"), among other e-mail accounts.

b. Defendant CHARLES UMEH CHIDI, a/k/a "Charlie," resided in the United Kingdom. Defendant CHIDI used the e-mail account Carl_Jay@[Provider 3].co.uk.

c. Defendant WAYA NWAKI, a/k/a "Jonh Done," a/k/a "Prince Abuja," a/k/a "Shawn Conley," a/k/a "USAPrince12k," resided in or near Atlanta, Georgia. Defendant NWAKI used the e-mail accounts usaprincele12k@[Provider 1].com and usaprincele12k@[Provider 2].com, among other e-mail accounts.

d. Defendant OSARHIEME UYI OBAYGBONA, a/k/a "Uyi Obaygbona," a/k/a "bside bside," resided in or near Atlanta, Georgia. Defendant OBAYGBONA used the e-mail account htownniggas@[Provider 2].com.

e. Defendant MARVIN DION HILL, a/k/a "Da Boss," a/k/a "Nihiar Springs," a/k/a "Nyhiar Da Boss," resided in or near College Park, Georgia. Defendant HILL used the e-mail accounts nahnahgetmoney@[Provider1].com and nyhiar@[Provider1].com.

f. Defendant ALPHONSUS OSUALA, a/k/a "Andrew Johnson," a/k/a "jamal j," resided in or near Atlanta, Georgia. Defendant OSUALA used the e-mail account aldandy_22@[Provider2].com.

g. Defendant OLANIYI JONES, a/k/a "Brenda Stuart," a/k/a "Olaniyi Victor Makinde," a/k/a "Makinde Olaniyi Victor," resided in Nigeria. Defendant JONES used the e-mail accounts bsbrendastuartbs@[Provider 1].com and brendastuart@[Provider

31.com, among other e-mail accounts.

Other Individuals

h. J.M., who is not charged as a defendant in this Indictment, resided in New York City. Defendant JONES, posing as "Brenda Stuart," e-mailed J.M. in order to deceive him into believing that "Brenda Stuart" was an American woman who was romantically interested in J.M. After receiving provocative and intimate e-mails and photographs from "Brenda Stuart," J.M. received and wired proceeds of the fraud to overseas bank accounts that defendant JONES controlled.

Corporations

i. Automated Data Processing, Inc., headquartered in Essex County, New Jersey ("ADP"); Intuit, Inc., headquartered in California ("Intuit"); and other payroll processing companies (collectively, "the Payroll Processors") provided outsourcing of human resources, payroll, tax and benefits administration services. The Payroll Processors offered customers the ability to manage their payroll accounts over the Internet. Upon providing the appropriate username and password (hereinafter, "Log-In Credentials") at the Payroll Processors' public-facing websites, customers could add employees to their payroll and pay those employees.

j. Ecount, a subsidiary of Citigroup, sold prepaid debit cards onto which employers, including customers of the

Payroll Processors, could transfer payroll amounts instead of using traditional paychecks or direct deposit ("Payroll Debit Cards").

k. Bank of America and JPMorgan Chase Bank ("Chase Bank") were financial institutions within the meaning of Title 18, United States Code, Section 20. Bank of America and Chase Bank were among the country's largest retail financial institutions and offered extensive consumer credit, checking, and savings products that provided customers online access to their accounts.

Definitions

1. In "phishing" attacks, online criminals create fraudulent websites and e-mails that mimic the legitimate websites and e-mails of e-Commerce providers (such as banks, payroll processors, and utilities) in an attempt to trick unwitting computer users – who believe that they are dealing with legitimate websites – into divulging their Log-In Credentials and other personally identifying information, such as dates of birth, Social Security Numbers, addresses, telephone numbers, mother's maiden names, and responses to online security questions ("Personal Identifiers"). The Log-In Credentials and Personal Identifiers, once stolen, can be used in furtherance of computer crimes that involve unauthorized access to online accounts.

m. "Spear phishing" attacks are phishing attacks

where online criminals select their victims using knowledge of the victims' existing account relationships. The attack depends upon the premise that impersonating communications from ADP, for example, is a far more effective tactic when communications are sent to ADP customers (a spear phishing attack) than if they are sent indiscriminately to employers nationwide (a phishing attack).

THE CONSPIRACY

5. Between in or about August 2009 and in or about June 2010, in the District of New Jersey and elsewhere, defendants

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing,"
CHARLES UMEH CHIDI,
a/k/a "Charlie,"
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"
a/k/a "Shawn Conley,"
a/k/a "USAPrince12k,"
OSARHIEME UYI OBAYGBONA,
a/k/a "Uyi Obaygbona,"
a/k/a "bside bside,"
MARVIN DION HILL,
a/k/a "Da Boss,"
a/k/a "Nyhiar Da Boss,"
a/k/a "Nihiar Springs,"
ALPHONSUS OSUALA,
a/k/a "Andrew Johnson,"
a/k/a "jamal j," and
OLANIYI JONES,
a/k/a "Brenda Stuart,"
a/k/a "Olaniyi Victor Makinde,"
a/k/a "Makinde Olaniyi Victor"

did knowingly and intentionally conspire with each other 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, to transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, and sounds, contrary to Title 18, United States Code, Section 1343.

OBJECT OF THE CONSPIRACY

6. It was the object of the conspiracy for defendants KARKLINS, CHIDI, NWAKI, OBAYGBONA, HILL, OSUALA, and JONES and others to steal money from payroll processors and banks by using phishing and spear phishing attacks to obtain Log-In Credentials and Personal Identifiers that were used to make unauthorized withdrawals from customers' online accounts.

MANNER AND MEANS OF THE CONSPIRACY

The Phishing Attacks

7. It was part of the conspiracy that defendants KARKLINS and CHIDI and others designed and deployed on the Internet fraudulent web pages ("Phishing Pages") that resembled the public-facing websites of payroll processing companies and banks ("the E-Commerce Companies").

8. It was further part of the conspiracy that defendants

KARKLINS and CHIDI and others caused phishing and spear phishing e-mails to be sent to the E-Commerce Companies' customers ("the Customers") in an attempt to trick the Customers into visiting the Phishing Pages. These e-mails appeared to be legitimate but were actually fraudulent e-mails that contained electronic links to the Phishing Pages. Those Customers who clicked on the electronic links were directed automatically to the Phishing Pages, where they saw what appeared to be the trademarked logos of the E-Commerce Companies and were prompted for and entered their Log-In Credentials and Personal Identifiers.

9. It was further part of the conspiracy that defendants KARKLINS and CHIDI and others caused any Log-In Credentials and Personal Identifiers that Customers typed into Phishing Pages to be intercepted and transmitted, not to the E-Commerce Companies, but to computers and e-mail accounts that defendants KARKLINS and CHIDI and others controlled.

Using the Stolen Log-In Credentials and Personal Identifiers

10. It was further part of the conspiracy that defendants KARKLINS, CHIDI, NWAKI, OBAYGBONA, HILL, and OSUALA and others emailed Log-In Credentials and Personal Identifiers that they had obtained to each other and others in exchange for payment or the promise of payment.

11. It was further part of the conspiracy that defendants KARKLINS, NWAKI, HILL, and others contacted the E-Commerce

Companies by telephone and over the Internet and used stolen Log-In Credentials and Personal Identifiers to impersonate the Customers and to obtain additional Personal Identifiers.

12. It was further part of the conspiracy that defendants KARKLINS and NWAKI and others used stolen Log-In Credentials and Personal Identifiers to cause fraudulent withdrawals to be made from the Customers' accounts at the E-Commerce Companies ("the Fraudulent Withdrawals").

Distributing the Proceeds of the Scheme

13. It was further part of the conspiracy that defendant KARKLINS and others caused some of the Fraudulent Withdrawals to be deposited onto Ecount Payroll Debit Cards and into other bank accounts that they controlled.

14. It was further part of the conspiracy that defendants KARKLINS and JONES and others caused the proceeds of some of the Fraudulent Withdrawals to be transferred to bank accounts belonging to individuals they employed ("Money Mules").

15. It was further part of the conspiracy that defendants KARKLINS and JONES caused the Money Mules to transfer funds out of the United States, sometimes by persuading the Money Mules that they were wiring money in furtherance of romantic relationships or professional opportunities.

16. It was further part of the conspiracy that defendants KARKLINS, CHIDI, NWAKI, HILL, JONES and others shared the

proceeds of the Fraudulent Withdrawals through wire transfers to individuals and bank accounts that they controlled in the United States, Mexico, the United Kingdom, Latvia, France, Bulgaria, Russia, and Nigeria, among other countries.

17. In this fashion, defendant KARKLINS, CHIDI, NWAKI, OBAYGBONA, HILL, OSUALA, and JONES and others attempted to obtain at least approximately \$3.5 million in Fraudulent Withdrawals, and did make at least approximately \$1.3 million in Fraudulent Withdrawals.

FRAUDULENT ACTIVITY

18. In order to further the object of the conspiracy, defendants KARKLINS, CHIDI, NWAKI, HILL, OBAYGBONA, OSUALA, and JONES and others conducted the following fraudulent activity in the District of New Jersey and elsewhere:

Phishing and Spear Phishing

a. On or about November 11, 2009, defendant KARKLINS e-mailed defendant CHIDI under the subject header "HOST INFO" ("the November 11 E-Mail"). The November 11 E-Mail contained Internet Protocol addresses, a user name, and a password that together provided administrative access (i.e., the ability to upload or download files over the Internet) to a computer located in Scranton, Pennsylvania that was used to store Phishing Pages and stolen Log-In Credentials and Personal Identifiers.

b. On or about November 12, 2009, defendant KARKLINS sent

an e-mail under the header "Chase Scam" ("the Chase Scam E-Mail") to the e-mail address lakes.sider80@[Provider1].com ("the Lakes Sider 80 Account"). The Chase Scam E-Mail contained an image of a Phishing Page resembling a public facing website of Chase Bank.

c. On or about November 12, 2009, defendant KARKLINS e-mailed the Lakes Sider 80 Account under the subject header "msg" ("the Msg E-Mail"). The Msg E-Mail attached a phishing e-mail that purported to come from Chase Bank requesting that customers "upgrade" their accounts "for security reasons" by clicking on an electronic link.

d. On or about December 9, 2009, defendant KARKLINS created an e-mail attaching the Chase Scam E-Mail and a Phishing Page that impersonated a public-facing website of Chase Bank.

e. On or about January 12, 2010, defendant KARKLINS created an e-mail containing a Phishing Page that impersonated a public-facing website of ADP.

f. On or about January 12, 2010, defendant KARKLINS created and sent three e-mails containing approximately 27 sets of ADP and e-mail Log-In Credentials under the subject header "ADPs from SPAM" and "ADP."

Attacks Targeting Payroll Processors and their Customers

The H.M. Transaction

g. On or about March 4, 2010, at approximately 12:09 a.m. (GMT), defendant KARKLINS e-mailed defendant NWAKI and instructed

him to telephone ADP and to impersonate "H.M.," the controller of ADP customer "Company A," and to request that ADP issue approximately \$69,000 in payroll checks to three purported Company A.O. employees: "M.G.," "E.W.," and "J.T."

h. Approximately 30 minutes later, defendant NWAKI e-mailed defendant HILL and instructed defendant HILL to telephone ADP, to impersonate H.M., and to cause ADP to issue approximately \$69,000 in payroll checks to M.G., E.W., and J.T. Defendant NWAKI instructed defendant HILL, in part:

Why u must call is that u must make her process the payroll for march 4. That's what u start the conversation wit..that u want to what to do to process the march 4 payrolls.

i. On or about March 4, 2010, defendants KARKLINS, NWAKI, and HILL and others accessed ADP's public-facing website and caused ADP to issue approximately \$60,000 in payroll on behalf of Company A.O. to M.G., E.W. and J.T., including by transferring approximately \$30,000 to an Ecount Payroll Debit Card in the name of J.T. ("the J.T. Ecount Card").

j. On or about March 4, 2010, defendants KARKLINS, NWAKI and HILL and others caused approximately \$30,000 to be wired from the J.T. Ecount Card to a Sovereign Bank account in the name of J.M. ("the J.M. Sovereign Account").

k. On or about March 8, 2010, defendant JONES caused J.M. to wire approximately \$26,500 from the J.M. Sovereign Account to an account at Ecobank, a Nigerian bank, that defendant JONES

controlled ("the Ecobank Account").

The D.C. Transaction

l. On or about February 16, 2010, defendant KARKLINS e-mailed Log-In Credentials associated with the payroll account of "Law Firm C," an ADP customer, to lakes.sider70@[Provider 1].com ("the Lakes Sider 70 Account").

m. On or about February 16, 2010, defendant KARKLINS and others caused ADP to initiate four fraudulent payroll transfers of approximately \$10,000, each on behalf of Law Firm C, to an Ecount Payroll Debit Card in the name of D.C., a purported employee who had been added to Law Firm C's payroll account at ADP ("the D.C. Ecount Card").

n. On or about February 17, 2010, defendant KARKLINS and others caused Ecount to transfer approximately \$40,000 from the D.C. Ecount Card to the J.M. Sovereign Account.

o. On or about February 18, 2010, the day after the funds arrived in the J.M. Sovereign Account, defendant JONES caused J.M. to wire approximately \$29,000 from the J.M. Sovereign Account to an account at Intercontinental Bank, a Nigerian bank, that defendant JONES controlled ("the Intercontinental Account").

p. On or about February 18, 2010, defendant KARKLINS exchanged e-mails with an attorney at Law Firm C in which defendant KARKLINS purported to seek legal advice regarding a pending criminal charge.

q. On or about February 21, 2010, defendant JONES forwarded to the Lakes Sider 70 Account an e-mail from J.M. reporting that J.M. had forwarded approximately \$29,000 to the Intercontinental Account.

The B.B. Transaction

r. On or about January 26, 2010, a coconspirator used the Lakes Sider 80 Account to create an e-mail containing the Log-In Credentials of an ADP customer, "Corporation D."

s. On or about January 28, 2010, a coconspirator used the Lakes Sider 80 Account to create an e-mail containing the Log-In Credentials and Personal Identifiers of an individual identified herein as "B.B."

t. On or about February 5, 2010, a coconspirator fraudulently caused ADP to wire, on behalf of its customer, Corporation D, approximately \$21,000 to an Ecount Payroll Debit Card in the name of B.B., a purported employee who had been added to Corporation D's payroll account at ADP ("the B.B. Ecount Card").

u. On or about February 8, 2010, a coconspirator transferred approximately \$21,700 to the J.M. Sovereign Account.

v. On or about February 11, 2010, defendant JONES caused J.M. to transfer approximately \$20,700 to the Ecobank Account.

w. On or about February 11, 2010, defendant JONES e-mailed to the Lakes Sider 80 Account confirmation of an approximately

\$20,700 wire transfer from the J.M. Sovereign Account.

Impersonating a Company F Representative

x. On or about March 11, 2010, defendant KARKLINS e-mailed an ADP client service manager. KARKLINS represented himself to be a representative of Company F, an ADP customer, inquiring why payroll had been suspended on Company F's account.

y. On or about March 11, 2010, a coconspirator fraudulently caused ADP to wire, on behalf of its customer Company F, approximately \$40,000 to an Ecount Payroll Debit Card in the name of J.H., a purported employee who had been added to Corporation F's payroll account at ADP.

The J.M. Sovereign Account Wire Confirmation

z. On or about October 21, 2009, defendant JONES caused J.M. to wire approximately \$13,400 obtained from Intuit from the J.M. Sovereign Account to the Ecobank Account ("the October 21 Wire").

aa. On or about October 23, 2009, an unknown coconspirator used the Lakes Sider 80 Account to e-mail defendant KARKLINS a scanned copy of a Sovereign Bank wire transfer confirming the October 21 Wire.

bb. Between in or about July 2009 and in or about April 2010, defendant JONES caused J.M. to send at least approximately

\$300,000 from the J.M. Sovereign Account to defendant JONES in Nigeria.

Attacks Targeting Banks

K.J.W.

cc. On or about September 17, 2009, defendant KARKLINS e-mailed defendant CHIDI the Log-In Credentials and Personal Identifiers of the Chase Bank customer "K.J.W." under the subject header "The Login!!! 30k lets make a lot \$\$\$\$."

dd. On or about September 21, 2009, defendants KARKLINS and CHIDI caused a Fraudulent Withdrawal of approximately \$13,000 from K.J.W.'s Chase Bank account.

ee. On or about November 18, 2009, defendant NWAKI e-mailed K.J.W.'s Log-In Credentials and Personal Identifiers to defendant OBAYGBONA under the subject header "Chase."

ff. On or about November 21, 2009, defendant KARKLINS e-mailed defendant NWAKI K.J.W.'s Log-In Credentials and Personal Identifiers under the subject header "28k chase, male, login yourself for check copy."

L.D.

gg. On or about October 21, 2009, defendant KARKLINS e-mailed defendant NWAKI under the subject header "Chase 23K Female with Check copy attached" ("the October 5 E-Mail"). The October 5 E-Mail contained Log-In Credentials, the Personal Identifiers,

and the bank account balance of "L.D." The October 5 E-Mail also attached an image of a check drawn on L.D.'s Chase Bank account.

hh. On or about October 21, 2009, defendant NWAKI e-mailed defendant HILL an image of the same check drawn on L.D.'s Chase Bank, L.D.'s Personal Identifiers and L.D.'s bank account balance.

ii. On or about October 22, 2009, defendants KARKLINS, NWAKI and HILL caused a Fraudulent Withdrawal of approximately \$5,000 from L.D.'s Chase Bank account.

R.R.

jj. On or about October 29, 2009, defendant KARKLINS e-mailed defendant NWAKI the Log-In Credentials and Personal Identifiers for the Chase Bank customer "R.R." and an image of a check drawn on R.R.'s Chase Bank account.

kk. On or about October 30, 2010, defendant KARKLINS and NWAKI caused a Fraudulent Withdrawal of approximately \$5,000 from R.R.'s Chase Bank checking account.

ll. On or about November 12, 2009, defendant NWAKI e-mailed R.R.'s Log-In Credentials, Personal Identifiers and an image of a check drawn on R.R.'s account to defendant OBAYGBONA.

K.M.

mm. On or about November 4, 2009, defendant KARKLINS e-mailed defendant NWAKI the Log-In Credentials and Personal Identifiers for the Chase Bank customer "K.M."

nn. On or about November 11, 2009, defendant NWAKI e-mailed K.M.'s Log-In Credentials and Personal Identifiers to defendant OBAYGBONA.

oo. On or about November 17, 2009, defendants KARKLINS, NWAKI, and OBAYGBONA caused a Fraudulent Withdrawal of approximately \$12,200 from K.M.'s Chase Bank account through purchases made at Atlanta-area retail stores.

S.M.

pp. On or about January 19, 2010, at approximately 8:00 p.m. (UTC), defendant NWAKI e-mailed defendant KARKLINS under the subject header "re: = CHASE 13.8k = male, age 32, check copy attached" the Log-In Credentials and Personal Identifiers of a Chase Bank customer named "S.M."

qq. On or about January 19, 2010, at approximately 11:30 p.m. (UTC), defendant KARKLINS created an e-mail under the subject header "2k Regions did to Wachovia [S.]" containing S.M.'s name and computer code evidencing unauthorized access to S.M.'s Chase Bank online account.

Gaining Unauthorized Access to Customers' Online Accounts

B.R.

rr. On or about November 15, 2009, defendant KARKLINS accessed an online Bank of America account belonging to "B.R.,"

and accessed screens related to "Safepass," an online security feature offered by Bank of America.

ss. That day, defendant KARKLINS sent an e-mail with the subject header "boa 26k + safepass added with the number u gave + mail access" to the Lakes Sider 80 Account that included Log-In Credentials and Personal Identifiers for "B.R.," including responses to the questions "What is your maternal grandmother's first name?" and "What is your mother's middle name?"

S.H.

tt. On or about December 30, 2009, defendant KARKLINS sent an e-mail under the header "boa business 25k + mail access" to AO7million@[Provider1].com containing the Log-In Credentials and Personal Identifiers of a Bank of America customer, "S.H.", including account balances and responses to Bank of America security questions.

uu. On or about December 31, 2009, defendant KARKLINS gained unauthorized access to S.H.'s online Bank of America account and attempted to send approximately \$4,500 by wire to a bank account in Mexico.

R.J.K.

vv. On or about January 20, 2010, defendant KARKLINS e-mailed defendant NWAKI under the subject header "@Chase@Male, 22k, age 54, check copy attached - find dob urself" ("the January

20 E-Mail"). The January 20 E-Mail contained the Log-In Credentials and bank balance of a Chase Bank customer, "R.J.K." Defendant KARKLINS also attached an image of a check drawn on R.J.K.'s Chase account to the January 20 E-Mail.

ww. In a reply to the January 20 E-Mail on or about January 21, 2010, defendant NWAKI stated, in substance and in part, "on this one you f*ck up again. i can login into the account cuz u give me the wrong email address" Defendant KARKLINS replied, in substance and in part, "You have lame hands. IT WORKS BITCH".

J.K.

xx. On or about March 18, 2010, defendant OSUALA sent an e-mail to defendant NWAKI that contained the Log-In Credentials and Personal Identifiers of a Chase Bank customer, "J.K."

yy. On or about April 7, 2010, at approximately 6:06 p.m., defendant NWAKI sent an e-mail under the header "New chase ass" to defendant KARKLINS that contained J.K.'s Log-In Credentials and Personal Identifiers.

zz. On or about April 7, 2010, at approximately 6:20 p.m., defendant KARKLINS accessed J.K.'s Chase Bank online account without authorization.

aaa. On or about May 25, 2010, J.K.'s Chase Bank account received a fraudulent \$24,000 ACH deposit from Citibank. That day and the next day, more than \$24,000 was withdrawn from J.K.'s

account by a coconspirator.

M.H.

bbb. On or about April 5, 2010, defendant NWAKI sent an e-mail to defendant KARKLINS under the header "he changed the usid use this account" that contained the Log-In Credentials of a Chase Bank customer, "M.H.," to defendant KARKLINS.

ccc. On or about April 6, 2010, defendant KARKLINS accessed M.H.'s Chase Bank online account without authorization.

C.M.

ddd. On or about March 12, 2010, defendant NWAKI created an e-mail under the subject header "[C.M.]" that contained the Log-In Credentials and Personal Identifiers of a Chase Bank customer, "C.M."

eee. On or about April 5, 2010, defendant KARKLINS accessed C.M.'s Chase Bank online account without authorization.

fff. On or about April 21, 2010, defendant KARKLINS created an e-mail under the header "Chase Drops" containing C.M.'s Log-In Credentials and Personal Identifiers.

ggg. On or about June 30, 2010, defendant KARKLINS created an e-mail under the header "Chase Drops" containing C.M.'s Log-In Credentials and Personal Identifiers.

Trafficking in the Log-In Credentials and Personal Identifiers of New Jersey Residents

hhh. On or about November 21, 2009, defendant KARKLINS e-mailed defendant NWAKI the Log-In Credentials and Personal Identifiers of "B.S.," a Chase Bank customer who resided in New Jersey.

iii. On or about December 7, 2009, defendant KARKLINS e-mailed defendant NWAKI the Log-In Credentials and Personal Identifiers of "A.O.," a Chase Bank customer who resided in New Jersey.

Harvesting Personal Identifiers

jjj. On or about April 8, 2010 at 1:33 (GMT), defendant HILL e-mailed five names and addresses of individuals residing in Alpharetta or Cumming, Georgia to defendant NWAKI.

kkk. Approximately four hours later, at 6:08 (GMT), defendant NWAKI e-mailed the same five names and addresses to defendant KARKLINS under the subject "Pls get the ssn# n dob."

Sharing the Proceeds of the Conspiracy

lll. On or about February 19, 2010, defendant HILL opened a bank account at Regions Bank ("the Hill Regions Account").

mmm. On or about March 30, 2010, defendant KARKLINS e-mailed defendant NWAKI instructions to wire approximately \$2,700 to Bulgaria and approximately \$925 to Latvia.

nnn. On or about March 30, 2010, defendant HILL wired approximately \$2,600 via Western Union to Bulgaria to a recipient named "D.N.R."

ooo. On or about March 30, 2010, defendant NWAKI e-mailed defendant KARKLINS that defendant HILL had wired approximately \$2,600 to D.N.R. in Bulgaria. Defendant NWAKI further advised that approximately \$830 in additional funds had been sent to "G.G.," a recipient in Latvia.

ppp. On or about March 31, 2010, defendant NWAKI e-mailed defendant KARKLINS under the subject header "50k drop" with the Log-In Credentials for the Hill Regions Account.

qqq. On or about May 14, 2010, under the subject header "WU info's," defendant KARKLINS sent the following e-mail to defendant NWAKI:

Send 4170 USD (deduct fee's from his share) to:
First name: [V.]
Last name: [V.]
City: Sofia
Country: Bulgaria

DON'T USE PRINCE ABUJA NAME FOR THIS !!! -> Send 1390
USD (deduct fees from his share) to:
First name: [E.]
Last name: [G.]
City: Riga
Country: Latvia

rrr. Between in or about September 2009 and in or about December 2010, defendant KARKLINS and others in Latvia (whose names defendant KARKLINS e-mailed to defendant NWAKI) received approximately \$98,000 via Western Union.

sss. Between in or about July 2009 and in or about April 2010, defendant JONES caused J.M. to send at least approximately \$300,000 from the J.M. Sovereign Account to defendant JONES in Nigeria.

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

COUNTS 2 THROUGH 5

18 U.S.C. § 1343

18 U.S.C. § 2

(Wire Fraud)

(Defendants KARKLINS, NWAKI, HILL and JONES)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. On or about the dates set forth below, in Essex County, in the District of New Jersey, and elsewhere, the defendants identified below and others did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud and to obtain money and property from the Payment Processors by means of materially false and fraudulent pretenses, representations, and promises, namely, through the manner and means described in paragraphs 7 through 17 of Count 1 of the Indictment, and for the purpose of executing such scheme or artifice, did knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely wire transfers from Sovereign Bank in the United States to various bank accounts in Nigeria in the approximate amounts described below.

COUNT	DEFENDANTS	DATE	AMOUNT	WIRE DESTINATION
2	KARKLINS NWAKI HILL JONES	03/08/2010	\$26,585	Ecobank
3	KARKLINS JONES	02/19/2010	\$28,334	Intercontinental

COUNT	DEFENDANTS	DATE	AMOUNT	WIRE DESTINATION
4	JONES	02/11/2010	\$20,692	Ecobank
5	KARKLINS JONES	10/21/2009	\$13,400	Ecobank

In violation of Title 18, United States Code, Section 1343
and Section 2.

COUNTS 6 THROUGH 9

18 U.S.C. § 1343

18 U.S.C. § 2

(Wire Fraud)

(Defendants KARKLINS, CHIDI, NWAKI, OBAYGBONA, and HILL)

1. Paragraphs 1 and 4 through 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. On or about the dates set forth below, in Essex County, in the District of New Jersey, and elsewhere, the defendants identified below and others did knowingly and intentionally devise and intend to devise a scheme and artifice to defraud and to obtain money and property from JPMorgan Chase Bank by means of materially false and fraudulent pretenses, representations, and promises, namely, through the manner and means described in paragraphs 7 through 17 of Count 1 of the Indictment, and for the purpose of executing such scheme or artifice, did knowingly transmit and cause to be transmitted by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures, and sounds, namely, interstate and international emails containing Log-In Credentials and Personal Identifiers of the bank customers identified below sent in furtherance of Fraudulent Withdrawals in the approximate amounts identified below:

Count	Defendants	Date	Accountholder	Fraudulent Withdrawal
6	KARKLINS CHIDI	09/17/2009	"K.J.W."	\$13,000

Count	Defendants	Date	Accountholder	Fraudulent Withdrawal
7	KARKLINS NWAKI HILL	10/21/2009	"L.D."	\$5,000
8	KARKLINS NWAKI	10/29/2009	"R.R."	\$5,000
9	OBAYGBONA KARKLINS NWAKI	11/17/2009	"K.M."	\$12,203.56

In violation of Title 18, United States Code, Section 1343
and Section 2.

COUNT 10

18 U.S.C. § 1028(f)
(Conspiracy to Commit Identity Theft)
(All Defendants)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. Between at least as early as in or about August 2009 and in or about June 2010, in the District of New Jersey and elsewhere, defendants

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing,"
CHARLES UMEH CHIDI,
a/k/a "Charlie,"
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"
a/k/a "Shawn Conley,"
a/k/a "USAPrince12k,"
OSARHIEME UYI OBAYGBONA,
a/k/a "Uyi Obaygbona,"
a/k/a "bside bside,"
MARVIN DION HILL,
a/k/a "Da Boss,"
a/k/a "Nyhiar Da Boss,"
a/k/a "Nihiar Springs,"
ALPHONSUS OSUALA,
a/k/a "Andrew Johnson,"
a/k/a "jamal j," and
OLANIYI JONES,
a/k/a "Brenda Stuart,"
a/k/a "Olaniyi Victor Makinde,"
a/k/a "Makinde Olaniyi Victor"

did knowingly and intentionally conspire with each other and others to transfer, possess and use means of identification of other persons without lawful authority, in a manner affecting interstate and foreign commerce, with the intent to commit, and

in connection with, unlawful activity constituting a violation of federal law, namely, Title 18, United States Code, Section 1343, contrary to Title 18, United States Code, Sections 1028(a)(7).

In violation of Title 18, United States Code, Section 1028(b)(1).

COUNTS 11 THROUGH 19

18 U.S.C. § 1028A(a)(1)

18 U.S.C. § 2

(Aggravated Identity Theft)

(Defendants KARKLINS, CHIDI, NWAKI, HILL, OBAYGBONA, and OSUALA)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. On or about the dates set forth below, in the District of New Jersey and elsewhere, the defendants identified below did knowingly and intentionally transfer, possess, and use, without lawful authority, means of identification of other persons, namely, the Log-In Credentials and Personal Identifiers of the individuals identified below, during and in relation to the felony violation of Title 18, United States Code, Section 1349, that is charged in Count 1 of this Indictment.

Count	Defendants	Date	Person
11	KARKLINS NWAKI HILL	03/04/2010	"H.M."
12	KARKLINS	02/16/2010	"Law Firm C"
13	KARKLINS CHIDI OBAYGBONA	09/17/2009 to 11/21/2009	"K.J.W."
14	KARKLINS NWAKI HILL	10/5/2009 to 10/21/2009	"L.D."
15	KARKLINS NWAKI OBAYGBONA	10/29/2009 to 11/12/2009	"R.R."

Count	Defendants	Date	Person
16	OBAYGBONA KARKLINS NWAKI	11/04/2009 to 11/11/2009	"K.M."
17	KARKLINS NWAKI	11/21/2009	"B.S."
18	KARKLINS NWAKI	12/07/2009	"A.O."
19	OSUALA NWAKI	03/18/2010	"J.K."

COUNT 20

18 U.S.C. § 1030(b)
(Conspiracy to Gain Unauthorized Access to Computers)
(Defendants KARKLINS, CHIDI, NWAKI,
OBAYGBONA, HILL, and OSUALA)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. Between at least as early as August 2009 and in or about June 2010, in the District of New Jersey, and elsewhere, defendants

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing,"
CHARLES UMEH CHIDI,
a/k/a "Charlie,"
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"
a/k/a "Shawn Conley,"
a/k/a "USAPrince12k,"
OSARHIEME UYI OBAYGBONA,
a/k/a "Uyi Obaygbona,"
a/k/a "bside bside,"
MARVIN DION HILL,
a/k/a "Da Boss,"
a/k/a "Nyhiar Da Boss,"
a/k/a "Nihiar Springs," and
ALPHONSUS OSUALA,
a/k/a "Andrew Johnson,"
a/k/a "jamal j"

did knowingly and with intent to defraud conspire and agree with each other and others to access protected computers without authorization, namely the computer networks used in and affecting interstate and foreign commerce and communication owned by Bank of America and JPMorgan Chase Bank, and exceed authorized access,

and by means of such conduct to obtain information for purposes of private financial gain and to further the intended fraud and obtain things of value, contrary to Title 18, United States Code, Sections 1030(a)(2)(C), (c)(2)(B)(i), and(a)(4).

In violation of Title 18, United States Code, Section 1030(b).

COUNTS 21 THROUGH 27
18 U.S.C. § 1030(a)(4)
18 U.S.C. § 2
(Unauthorized Access to Computers to Commit Fraud)
(Defendants KARKLINS and NWAKI)

1. Paragraphs 1 through 4 and 7 through 18 of Count 1 of this Indictment are realleged as if set forth herein.

2. On or about the dates set forth below, in Essex County, in the District of New Jersey, and elsewhere, defendants

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing," and
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"
a/k/a "Shawn Conley,"
a/k/a "USAPrince12k"

did knowingly and with intent to defraud access protected computers, namely the computer networks used in and affecting interstate and foreign commerce and communication owned by the banks identified below, without authorization, and exceeded authorized access, and by means of such conduct furthered the intended fraud and obtained things of value, namely Fraudulent Withdrawals from customers' accounts:


Count	Defendant	Victim Accountholder	Victim Bank	Date
21	KARKLINS	"B.R."	Bank of America	11/15/09
22	KARKLINS	"S.H."	Bank of America	12/30/09

23	KARKLINS NWAKI	"S.M."	Chase Bank	01/19/10
24	KARKLINS NWAKI	"R.J.K."	Chase Bank	01/20/10
25	KARKLINS	"C.M."	Chase Bank	04/05/10
26	KARKLINS NWAKI	"M.H."	Chase Bank	04/06/10
27	KARKLINS NWAKI	"J.K."	Chase Bank	04/07/10

In violation of Title 18, United States Code, Sections
1030(a)(4) and 1030(c)(3)(A) and Section 2.

A TRUE BILL

FOREPERSON



PAUL J. FISHMAN
United States Attorney

I HEREBY CERTIFY that the above and
foregoing is a true and correct copy of
the original on file in my office.

ATTEST
WILLIAM T. WALSH, Clerk
United States District Court
District of New Jersey

By: 
Deputy Clerk

CASE NUMBER: 11-CR-299(WJM)

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA

v.

KARLIS KARKLINS,
a/k/a "Susanne O'Neill,"
a/k/a "Kris,"
a/k/a "Steven Bing,"
CHARLES UMEH CHIDI,
a/k/a "Charlie,"
WAYA NWAKI,
a/k/a "Jonh Done,"
a/k/a "Prince Abuja,"

a/k/a "Shawn Conley,"
a/k/a "USAPrince12k,"
OSARHIEME UYI OBAYGBONA,
a/k/a "Uyi Obaygbona,"
a/k/a "bside bside,"
MARVIN DION HILL,
a/k/a "Da Boss,"
a/k/a "Nyhiar Da Boss,"
a/k/a "Nihiar Springs,"

ALPHONSUS OSUALA,
a/k/a "Andrew Johnson,"
a/k/a "jamal j," and
OLANIYI JONES,
a/k/a "Brenda Stuart,"
a/k/a "Olaniyi Victor
Makinde,"
a/k/a "Makinde Olaniyi
Victor"

INDICTMENT FOR VIOLATIONS OF

18 U.S.C. §§ 1343, 1349, 1028(f), 1028A(a)(1), 1030(a)(4), 1030(b) and 2

A True Bill,

Foreperson

PAUL J. FISHMAN


UNITED STATES ATTORNEY, NEWARK, NEW JERSEY

SETH B. KOSTO
ASSISTANT U.S. ATTORNEY
NEWARK, NEW JERSEY
(973) 645-2737

I HEREBY CERTIFY that the above and foregoing is a true and correct copy of the original on file in my office.

ATTEST

WILLIAM T. WALSH, Clerk
United States District Court
District of New Jersey

By: 
Deputy Clerk