IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF MISSISSIPPI
SOUTHERN DIVISION

UNITED STATES OF AMERICA

v.

CRIMINAL NO. 1:14cr33HSO-JMR

OLADIMEJI SEUN AYELOTAN,
TESLIM OLAREWAJU KIRIJI,
RASAQ ADEROJU RAHEEM,
DENNIS BRIAN LADDEN,
ADEKUNLE ADEFILA,
RHULAUNE FIONAH HLUNGWANE,
OLASUPO MOFOLUWASHO ODEBUNMI,
GENOVEVA FARFAN,
GABRIEL OLUDARE ADENIRAN,
SUSAN ANN VILLENEUVE,
OLUSEGUN SEYI SHONEKAN,
TAOFEEQ OLAMILEKAN OYELADE,
ODUNTAN SIKIRU LAWANI,
SESAN OLUMIDE FARIN,
OLUFEMI OBARO OMORAKA,
FEMI ALEXANDER MEWASE, and
ANUOLUWAPO SEGUN ADEGBEMIGUN

18 U.S.C. § 1349
18 U.S.C. § 371
18 U.S.C. § 1341

The Grand Jury charges:

At all times relevant to this indictment

1. N.J. was a resident of Harrison County in the Southern Division of the Southern District of Mississippi.
2. C.B. was a resident of Greene County in the Southern District of Mississippi.
3. M.M. was a resident of Jefferson County in the Southern District of Mississippi.
4. L.E. was a resident of Leake County in the Southern District of Mississippi.
5. N.E. was a resident of Leake County in the Southern District of Mississippi.

6. J.S. was a resident of Harrison County in the Southern Division of the Southern District of Mississippi.
7. J.B. was a resident of Covington County in the Southern District of Mississippi.
8. Hancock Bank was a financial institution in the Southern Division of the Southern District of Mississippi, the accounts and deposits of which were insured by the Federal Deposit Insurance Corporation. Hancock Bank was an organization whose normal activities took place in interstate and foreign commerce and which had an effect on interstate and foreign commerce.
9. Trustmark National Bank was a financial institution in the Southern District of Mississippi, the accounts and deposits of which were insured by the Federal Deposit Insurance Corporation. Trustmark National Bank was an organization whose normal activities took place in interstate and foreign commerce and which had an effect on interstate and foreign commerce.
10. American Express was a money service business duly registered with the Financial Crimes Enforcement Network authorized to act as a money service business and licensed and/or registered within the various states in which American Express does business.
11. Seniorpeoplemeet.com was an internet dating service whose normal activities took place in interstate and foreign commerce and which had an effect on interstate and foreign commerce.
12. Google, Inc. was an internet service provider whose normal activities took place in interstate and foreign commerce and which had an effect on interstate and foreign commerce.
13. Yahoo, Inc. was an internet service provider whose normal activities took place in interstate and foreign commerce and which had an effect on interstate and foreign commerce.

14. Personal Identification Information (hereinafter "PII") includes, but is not limited to, name, date of birth, address, social security number, bank account numbers, bank routing numbers, and any other name or number that may be used alone or in conjunction with any other information to identify a specific individual.

15. **OLADIMEJI SEUN AYELOTAN** is a citizen of Nigeria residing in South Africa who controlled and utilized the email accounts STACYADAMS20009@YAHOO.COM GLENNSATTELBERG1961@GMAIL.COM, EMPLOYMENTOFFERS007@YAHOO.COM, and OLADIMEJISEUN2008@YAHOO.COM.

16. **TESLIM OLAREWAJU KIRIJI** is a citizen of Nigeria residing in the United States who controlled and utilized the email account TESCOSG@YAHOO.COM.

17. **RASAQ ADEROJU RAHEEM** is a citizen of Nigeria residing in South Africa who controlled and utilized the email accounts SPOWELL26AL@GMAIL.COM, GERVINOJ11@GMAIL.COM, GERVINOJ@YAHOO.COM, JOHNVINO56@GMAIL.COM, RASAQ_ADEROJU@YAHOO.COM, KEVINSMITH3949@YAHOO.COM.

18. **DENNIS BRIAN LADDEN** is a citizen of the United States residing in Wisconsin who controlled and utilized the email account LUVNHANDS1940@YAHOO.COM.

19. **ADEKUNLE ADEFILA** is a citizen of Nigeria residing in Canada who controlled and utilized the email account PETERLAWSON5050@YAHOO.COM.

20. **RHULANE FIONAH HLUNGWANE** is a citizen of South Africa residing in South Africa.

21. **OLASUPO MOFOLUWASHO ODEBUNMI** is a citizen of Nigeria residing in South Africa who controlled and utilized email account JUSTIN.WORSHAM@YAHOO.COM.

22. **GENOVEVA FARFAN** is a citizen of the United States residing in California who controlled and utilized email account FNCYJEN@YAHOO.COM.

23. **GABRIEL OLUDARE ADENIRAN** is a citizen of Nigeria residing in South Africa who controlled and utilized email accounts MATTMILLER4070@GMAIL.COM. GENTILEMARK186@GMAILCOM and LLOYDFARELL0012008@YAHOO.COM.

24. **SUSAN ANN VILLENUEVE** is a citizen of the United States residing in California who controlled and utilized email account SUSANV1418@YAHOO.COM.

25. **OLUSEGUN SEYI SHONEKAN** is a citizen of Nigeria residing in South Africa who controlled and utilized email account MIMICOLE001@YAHOO.COM.

26. **TAOFEEQ OLAMILEKAN OYELADE** is a citizen of Nigeria residing in South Africa who controlled and utilized email account JONES_DICKSON@YAHOO.COM.

27. **ODUNTAN SIKIRU LAWANI** is a citizen of Nigeria residing in South Africa who controlled and utilized email accounts STARENTERPRISE74@YAHOO.COM and MAXWELLSAMUEL59@YAHOO.COM.

28. **SESAN OLUMIDE FARIN** is a citizen of Nigeria residing in South Africa who controlled and utilized email account OLUWA_NISHOLA@YAHOO.COM.

29. **OLUFEMI OBARO OMORAKA** is a citizen of Nigeria residing in South Africa who controlled and utilized email account FEMI_OMORAKA@YAHOO.COM and ADDIEP01@YAHOO.COM.

30. **FEMI ALEXANDER MEWASE** is a citizen of Nigeria residing in South Africa who controlled and utilized email account FMPLUST12@GMAIL.COM.

31. **ANUALUWAPO SEGUN ADEGBEMIGUN** is a citizen of Nigeria residing in South Africa who controlled and utilized email account SEGSEA121@YAHOO.COM.

32. A known co-conspirator is a citizen of Nigeria residing in Nigeria who controlled and utilized email account REDARMY_TX_HOST@YAHOO.COM.

33. A known co-conspirator is a citizen of Nigeria residing in Nigeria who controlled and utilized email account FAYEKIMBERLY@YMAIL.COM.

34. A known co-conspirator is a citizen of Nigeria residing in Nigeria who controlled and utilized email accounts FOLLYEDWARDS@YAHOO.COM and KAREN_ROB01@YAHOO.COM.

COUNT 1

Paragraphs 1 through 34 of this indictment are re-alleged and incorporated by reference as if fully set forth herein.

35. Beginning in at least 2001, and continuing until the date of this indictment, in Harrison County, in the Southern Division of the Southern District of Mississippi and elsewhere, the defendants, **OLADIMEJI SEUN AYELOTAN, TESLIM OLAREWAJU KIRIJI, RASAQ ADEROJU RAHEEM, DENNIS BRIAN LADDEN, ADEKUNLE ADEFILA, RHULANE FIONAH HLUNGWANE, OLASUPO MOFOLUWASHO ODEBUNMI, GENOVEVA FARFAN, GABRIEL OLUDARE ADENIRAN, SUSAN ANN VILLENEUVE, OLUSEGUN SEYI SHONEKAN, TAOFEEQ OLAMILEKAN OYELADE, ODUNTAN SIKIRU LAWANI, SESAN OLUMIDE FARIN, OLUFEMI OBARO OMORAKA, FEMI ALEXANDER MEWASE, and ANUOLUWAPO SEGUN ADEGBEMIGUN,** did knowingly and willfully conspire with each other and with others known and unknown to the grand jury, to violate the following sections of the United States Code:

36. a. Section 1341, Title 18 United States Code, that is, having devised and intended to devise a scheme and artifice to defraud and to obtain money or property by means of false and fraudulent pretenses and representations, and promises, and for the purpose of executing and attempting to execute such scheme and artifice, knowingly and unlawfully causes to be delivered by the United States Postal Service and private and interstate commercial carriers matters according to the directions thereon;

b. Section 1343, Title 18 United States Code, that is, having devised or intended to devise a scheme and artifice to defraud and to obtain money and property by means of false and fraudulent pretenses and representations, and promises, transmits or causes to be transmitted in interstate and foreign commerce certain wire communications for the purpose of executing the scheme or artifice;

c. Section 1344, Title 18 United States Code, that is, to knowingly execute or attempt to execute a scheme and artifice to obtain funds under the custody and control of financial institutions by means of false and fraudulent pretenses and representations.

37. It was the object of the conspiracy for the defendants, **AYELOTAN, KIRIJI, RAHEEM, LADDEN, ADEFILA, HLUNGWANE, ODEBUNMI, FARFAN, ADENIRAN, VILLENEUVE, SHONEKAN, OYELADE, LAWANI, FARIN, OMORAKA, MEWASE, and ADEGBEMIGUN,** and others, to unlawfully enrich themselves by conducting multiple complex financial fraud schemes via the internet. The various fraud schemes included internet romance scams, fraudulent check scams; bank and credit card account take overs, and work at home scams. The proceeds of these scams, both money and goods, were shipped from the United States to Pretoria, South Africa and various location in Nigeria through a complex re-shipping network of both complicit and unwitting individuals recruited through the various internet scams.

38. The object of the conspiracy was to be accomplished by the following manner and means:

39. It was a part of the conspiracy that the defendants, **AYELOTAN, KIRIJI, RAHEEM, LADDEN, ADEFILA, HLUNGWANE, ODEBUNMI, FARFAN, ADENIRAN, VILLENEUVE, SHONEKAN, OYELADE, LAWANI, FARIN, OMORAKA, MEWASE, and ADEGBEMIGUN,** would seek out and identify potential victims through online romance scams and work at home opportunities. Online dating sites were used to solicit potential victims through the use of mass e-mailings to users of the dating websites. Mass e-mailings were also used to solicit victims through the work at home scams.

40. It was a part of the conspiracy that the defendants, **AYELOTAN, KIRIJI, RAHEEM, LADDEN, ADEFILA, HLUNGWANE, ODEBUNMI, FARFAN, ADENIRAN, VILLENEUVE, SHONEKAN, OYELADE, LAWANI, FARIN, OMORAKA, MEWASE, and ADEGBEMIGUN,** would carry on a fictitious online romantic relationship with the victims in order to convince them to carry out various acts that furthered the objectives of the conspiracy. These acts included, among other things, receiving and shipping merchandise obtained with stolen PII and compromised credit card and banking information, depositing counterfeit checks, and transferring the proceeds of the conspiracy via wire transfer, U.S. Mail, and express package delivery services.

41. It was a part of the conspiracy that the defendants, **AYELOTAN, KIRIJI, RAHEEM, LADDEN, ADEFILA, HLUNGWANE, ODEBUNMI, FARFAN, ADENIRAN, VILLENEUVE, SHONEKAN, OYELADE, LAWANI, FARIN, OMORAKA, MEWASE, and ADEGBEMIGUN,** would obtain stolen PII, compromised credit card and banking information by purchasing it from underground forums which were operated by individuals engaged in the theft and sale of PII, more commonly known as "hackers." The stolen PII, compromised credit card and banking information would be used to fraudulently obtain credit cards, cellular telephone accounts, and pre-paid debit cards. These cards and accounts would be used to obtain cash and things of value, such as smartphones, tablets, computers and other types of electronics, most if which would be shipped internationally to Pretoria, South Africa for the benefit of the defendant's and their co-conspirators.

42. In order to accomplish the object of the conspiracy, the defendants, **AYELOTAN, KIRIJI, RAHEEM, LADDEN, ADEFILA, HLUNGWANE, ODEBUNMI, FARFAN, ADENIRAN, VILLENEUVE, SHONEKAN, OYELADE, LAWANI, FARIN, OMORAKA, MEWASE, and ADEGBEMIGUN,** and their co-conspirators committed the following acts in furtherance of the conspiracy, including but not limited to:

43. On or about November 25, 2001, email account TESCOSG@YAHOO.COM was created by defendant **KIRIJI** or an unknown co-conspirator.

44. On or about January 27, 2007, email account FAYEKIMBERLY@YMAIL.COM was created by a known or unknown co-conspirator.

45. On or about May 24, 2007, email account REDARMY_TX_HOST@YAHOO.COM was created by a known or unknown co-conspirator.

46. On or about January 08, 2008, email account TOYAGILMORE@YAHOO.COM was created by a known or unknown co-conspirator.

47. On or about January 08, 2008, email account SPOWELL26AL@GMAIL.COM was created by defendant **RAHEEM** or an unknown co-conspirator.

48. On or about August 25, 2011, email account GERVINOJ11@GMAIL.COM was created by defendant **RAHEEM** or an unknown co-conspirator.

49. On or about June 10, 2012, email account JOHNVINO56@GMAIL.COM was created by defendant **RAHEEM** or an unknown co-conspirator.

50. On or about March 23, 2006, email account PETERLAWSON5050@YAHOO.COM was created by defendant **ADEFILA** or an unknown co-conspirator.

51. On or about June 13, 2008, email account FOLLYEDWARDS@YAHOO.COM was created by a known or unknown co-conspirator.

52. On or about April 2, 2009, email account MATTMILLER4070@GMAIL.COM was created by defendant **ADENIRAN** or an unknown co-conspirator.

53. On or about August 13, 2010, email account SUSANV1418@YAHOO.COM was created by defendant **VILLENEUVE** or an unknown co-conspirator.

54. On or about April 29, 2007, email account KAREN_ROB01@YAHOO.COM was created by a known or unknown co-conspirator.

55. On or about June 30, 2012, email account GENTILEMARK186@GMAIL.COM was

created by defendant **ADENIRAN** or an unknown co-conspirator.

56. On a date unknown to the grand jury, email account LLOYDFARELL0012008@YAHOO.COM was created by defendant **ADENIRAN** or an unknown co-conspirator.

57. On or about September 28, 2009, email account STACYADAMS20009@YAHOO.COM was created by defendant **AYELOTAN** or an unknown co-conspirator.

58. On or about February 21, 2007, email account MIMICOLE001@YAHOO.COM was created by defendant **SHONEKAN** or an unknown co-conspirator.

59. On or about May 21, 2011, email account JONES_DICKSON@YAHOO.COM was created by defendant **OYELADE** or an unknown co-conspirator.

60. On or about October 27, 2007, email account STARENTERPRISE74@YAHOO.COM was created by defendant **LAWANI** or an unknown co-conspirator.

61. On or about October 4, 2011, email account MAXWELLSAMUEL59@YAHOO.COM was created by defendant **LAWANI** or an unknown co-conspirator.

62. On or about November 21, 2007, email account KEVINSMITH3949@YAHOO.COM was created by defendant **RAHEEM** or an unknown co-conspirator.

63. On a date unknown to the grand jury, email account EMPLOYMENTOFFERS007@YAHOO.COM was created by defendant **AYELOTAN** or an unknown co-conspirator.

64. On or about September 20, 2003, email account RASAQ_ADEROJU@YAHOO.COM was created by defendant **RAHEEM** or an unknown co-

conspirator.

65. On or about December 9, 2004, email account FEMI_OMORAKA@YAHOO.COM was created by defendant **OMORAKA** or an unknown co-conspirator.

66. On or about January 14, 2010, email account OLUWA_NISHOLA@YAHOO.COM was created by defendant **FARIN** or an unknown co-conspirator.

67. On or about February 14, 2010, email account FMPLUST12@GMAIL.COM was created by defendant **MEWASE** or an unknown co-conspirator.

68. On or about September 14, 2012, email account ADDIEP01@YAHOO.COM was created by defendant **OMORAKA** or an unknown co-conspirator.

69. On or about July 1, 2007, email account JUSTIN.WORSHAM@YAHOO.COM was created by defendant **ODEBUNMI** or an unknown co-conspirator.

70. On or about October 13, 2008, email account SEGSEA12@YAHOO.COM was created by defendant **ADEGBEMIGUN** or an unknown co-conspirator.

71. On a date unknown to the grand jury email account OLADIMEJISEUN2008@YAHOO.COM was created by defendant **AYELOTAN** or an unknown co-conspirator.

72. On or about December 26, 2006, email account JAMES_GERRALD247@YAHOO.COM was created by an unknown co-conspirator.

73. On or about July 22, 2012, email account KERRIWHITE840@YAHOO.COM was created by a co-conspirator known to the grand jury as "femi."

74. On or about October 28, 2011, email account GLENNSATTELBERG1961@GMAIL.COM was created by defendant **AYELOTAN** or an unknown co-conspirator.

75. On a date unknown to the grand jury email account FNCYJEN@YAHOO.COM was created by defendant **FARFAN** or an unknown co-conspirator.

76. The following acts in furtherance relate to the fraudulent takeover of the Capital One credit card account of victim J.S.

a. On or about October 16, 2012, a known co-conspirator sent an email to another known co-conspirator wherein he provided a known co-conspirator with the name and two addresses for defendant **LADDEN**.

b. On or about October 16, 2012, defendant **KIRIJI** made multiple telephone calls to Capital One from phone number 234 8055774218 for the purpose of fraudulently ordering a balance transfer check in the amount of $5,400 and having the fraudulently obtained check mailed to N15764 Sugar Bush Road, Park Falls, WI 54552-7617.

c. On or about October 18 and 19, 2012, a known co-conspirator engaged in a Yahoo! Messenger chat session with an unknown co-conspirator wherein the known co-conspirator tells the unknown co-conspirator that he is expecting a balance transfer check from Capital One Bank, and that he will need someone to sign the check, write a payee name on the check, and to cash the check.

d. On or about October 25, 2012, defendant **LADDEN** emailed a copy of the fraudulent balance transfer check to a known co-conspirator.

e. On or about October 25, 2012, a known co-conspirator forwarded the email containing the copy of the fraudulent balance transfer check from defendant **LADDEN** to defendant **RAHEEM** and a known conspirator. The email to defendant **RAHEEM** contained instructions to send the check back to defendant **LADDEN** at N15764 Sugar Bush Road, Park Falls, WI 54552-7617.

f. On or about October 26, 2012, defendant **RAHEEM** emailed the fraudulent balance transfer check to who he believed to be victim N.J. and instructed her to type the name and address of defendant **LADDEN** onto the front of the check using a typewriter, and to mail the check to the defendant **LADDEN**.

g. On or about October 27, 2012, defendant **RAHEEM** shipped the fraudulent balance transfer check via United Parcel Service to the home of victim N.J. in Biloxi, Mississippi.

h. On or about October 31, 2012, a known co-conspirator communicated via email and Yahoo! Messenger, with a person he believed to be the defendant **LADDEN** wherein a known co-conspirator directed who he believed to be defendant **LADDEN** to deposit the fraudulent balance transfer check into defendant **LADDEN's** Wells Fargo bank account, and to await further instructions.

i. On or about November 2, 2012, a known co-conspirator directed who he believed to be defendant **LADDEN**, via email, to withdraw $2,180 of the fraudulently obtained funds from defendant **LADDEN's** bank account and to deposit those funds into an account held at Bank of America, ending in number 0835, and belonging to victim R.T.

j. On or about November 3, 2012, a known co-conspirator directed who he believed to be defendant **LADDEN** via email to deposit the remaining $3,100 in fraudulently obtained funds into an account held at Bank of America, ending in number 7859.

k. On or about November 3, 2012, defendant **RAHEEM** informed victim R.T., via email, that $2,180 had been deposited into his/her Bank of America checking account, and that R.T. should withdraw $1,853 and transfer that amount via Money Gram wire transfer to an individual located in the Republic of Benin. Defendant **RAHEEM** also instructed R.T. to transfer $277 via Money Gram wire transfer to defendant **HLUNGWANE** in Pretoria, South Africa.

77. The following acts in furtherance relate to the fraudulent takeover of the Bank of America credit card account of victim J.K.

a. On or about November 14, 2012, defendant **KIRIJI** received an email containing the subject line "J.K. Jr. call D BOA inside Asap," the narrative portion of the email contained an online personal credit report from Experian for victim J.K. including his/her Bank of America credit card number.

b. On or about December 17, 2012, an unknown co-conspirator sent an email to a known co-conspirator that contained the name "San Bryant" and the address 200 Lilac Drive, Summerville, SC.

c. On or about December 17, 2012, a known co-conspirator contacted Bank of America and after providing J.K.'s identification verification information, directed Bank of America to add an authorized user named "San Bryant" to J.K.'s account and directed Bank of America to change the address on the account from J.K.'s address in Pennsylvania to 200 Lilac Drive, Summerville, SC. The known co-conspirator directed Bank of America to mail a new credit card to the South Carolina address.

d. On or about January 3 and 4, 2013, a known co-conspirator and unknown co-conspirator corresponded via Yahoo! Messenger wherein the unknown co-conspirator confirmed that he/she had received the new credit card for San Bryant. The known co-conspirator gave directions to an unknown co-conspirator on how to go about getting cash advances off of the fraudulent credit card and where to spend the money and what electronic goods to purchase with the fraudulently obtained funds.

e. On or about January 4 and 5, 2013, a known co-conspirator instructed an unknown co-conspirator to wire some of the proceeds from the fraudulently obtained cash advances to various persons, including defendants **KIRIJI** and **ADEFILA**.

78. The following acts in furtherance relate to the fraudulent takeover of the TD Ameritrade account of victims G.A. and A.A.

a. On or about September 1, 2013, a known co-conspirator sent an email to defendant **ADEFILA** which contained the PII of approximately 200 different individuals, including the PII of the victim G.A.

b. From on or about October 14, 2013 to on or about November 1, 2013, defendant **ADEFILA** called TD Ameritrade approximately 38 times representing himself to be the

victim G.A. During one of these calls, defendant **ADEFILA** requested an ACH bank setup form.

c. On or about October 3, 2013, defendant **ADEFILA** received an email from an unknown co-conspirator that contained a Wells Fargo bank account and routing number, along with the name of the account owner, and his online banking username, password and PIN. This account ended in number 9968.

d. On or about October 17, 2013, co-conspirators sent a completed Automated Clearing House (hereinafter "ACH") bank setup form along with a voided check to TD Ameritrade to connect the TD Ameritrade account owned by victims G.A. and A.A. with a Wells Fargo account ending in number 9968.

e. On or about October 28, 2013, co-conspirators caused an ACH transfer in the amount of $34,950 from the TD Ameritrade account into the Wells Fargo account ending in 9968.

f. On or about October 28, 2013, defendant **ADEFILA** sent an email to an unknown co-conspirator that contained a Citibank account ending in 7065.

g. On or about October 29, 2013, co-conspirators sent an ACH bank setup form along with a voided check to TD Ameritrade to connect the TD Ameritrade account owned by victims G.A. and A.A. with a Citibank account ending in number 7065.

h. On or about November 1, 2013, co-conspirators ordered an ACH transfer in the amount of $33,480 from the TD Ameritrade account into the Citibank account ending in 7065.

79. The following acts in furtherance relate to the fraudulent takeover of the Lincoln Financial Securities account of victims E.K. and R.K.

a. On or about August 17, 2013, a known co-conspirator sent an email to defendant **ADEFILA** which contained the PII of approximately 100 different individuals, including the PII of the victims E.K.

b. On or about October 1, 2013, defendant **ADEFILA** received an email from an unknown co-conspirator that contained a Wells Fargo bank account and routing number, along

with the name of the account owner, and his/her online banking username, password and PIN. This account ended in number 1082.

c. On or about October 9, 2013, defendant **ADEFILA** made several calls to Lincoln Financial Securities representing himself to be victim E.K. and providing E.K.'s social security number as a means of verification. During the calls, defendant **ADEFILA** inquired about the balance of the account, and asked for the number to which he could fax a wire transfer request.

d. On or about October 10, 2013, Lincoln Financial Securities received a wire transfer request via fax directing it to transfer $30,000 from the account belonging to victims E.K. and R.K. to an account held at Wells Fargo ending in number 1082. Prior to executing the transfer, Lincoln Financial Services contacted the trustee for E.K. and R.K., who verified that the wire transfer request was fraudulent.

80. The following acts in furtherance relate to the counterfeiting of a check made payable to N.J. in Biloxi, Mississippi.

a. On or about December 11, 2011, a known co-conspirator sent an email to defendant **VILLENEUVE** that contained the names and mailing addresses of approximately 51 different individuals, including the name and address of N.J. In this email, the known co-conspirator listed a dollar amount next to each name. $3,000 was listed next to the name and address of N.J.

b. On or about December 14, 2011, defendant **RAHEEM** sent at least three emails to N.J. that contained instructions for receiving a $3,000 check via FedEx mail. Defendant **RAHEEM** provided N.J. with the FedEx tracking number associated with the check, instructed her on how to deposit the check, to transfer the proceeds via Western Union wire transfer, and confirmed to her that the check was ready for pickup.

c. On or about December 14, 2011, co-conspirators caused the check payable to N.J. to be delivered to a person they believed was N.J.

81. The following acts in furtherance relate to the counterfeiting of a check made payable to C.B.

a. On or about August 26, 2012, defendant **ADENIRAN** sent an email to a known co-conspirator which contained three names and mailing addresses, including the name and address of C.B.

b. On or about August 26, 2012, a known co-conspirator sent an email to defendant **VILLENEUVE** which contained the names and mailing addresses of approximately 52 different individuals, including the name and address of C.B. In this email, a known co-conspirator listed a dollar amount next to each name. $3,550 was listed next to the name and address of C.B. This email also contained the routing and account numbers for an account held at Regions Bank, as well as the number of a check, 820193.

c. Between August 26, 2012 and September 5, 2012, co-conspirators caused items to be sent by the United States Postal Service or private or commercial interstate carrier to C.B. in Lucedale, Mississippi.

d. On or about September 8, 2012, defendant **ADENIRAN** and a known co-conspirator corresponded via Yahoo! Messenger wherein they discussed how the counterfeit check made payable to C.B. should be transferred from C.B. to a known co-conspirator via Money Gram.

e. On or about September 9, 2012, defendant **ADENIRAN** sent an email to C.B. wherein he provided the name and location of an individual in the Philippines.

f. On or about September 9, 2012, C.B. sent an email to defendant **ADENIRAN** wherein he/she provides defendant **ADENIRAN** with the claim number for the Money Gram wire transfer for $3,325 to the individual in the Philippines.

g. On or about September 10, 2012, defendant **ADENIRAN** sent an email to an individual living in the Philippines wherein he provided him/her with directions for receiving the Money Gram wire transfer for $3,325 from C.B., and for forwarding the proceeds to a known co-

conspirator.

82. The following acts in furtherance relate to the interstate shipping of merchandise obtained with the stolen PII and the compromised credit and bank accounts of victims D.G. and J.S.

a. On or about September 26, 2011, co-conspirators caused a fraudulent AT&T wireless account to be opened utilizing the PII of victim D.G.

b. Immediately after creating the fraudulent D.G. AT&T account, co-conspirators purchased two BlackBerry Torch smartphones using a Visa credit card ending in 9506 stolen from victim J.S., which were then shipped to the home of victim N.J. in Biloxi, Mississippi.

c. On or about September 28, 2011, defendant **AYELOTAN** sent an email to defendant **RAHEEM**, which contained multiple shipping labels purchased from the United States Postal Service with a compromised credit card. These shipping labels were used to re-ship the BlackBerry Torch smartphones from Biloxi, Mississippi to Pretoria, South Africa.

d. On or about September 28, 2011, defendant **RAHEEM** forwarded the email with the shipping labels to N.J. and instructions to N.J. on how to re-ship the fraudulently obtained smartphones to Pretoria, South Africa.

e. On or about September 29, 2011, N.J. reported the package and emails to law enforcement.

83. The following acts in furtherance relate to the interstate shipping of merchandise obtained with the stolen PII and the compromised credit and bank accounts of victims A.S. and J.H.

a. On or about February 26, 2012, co-conspirators caused a fraudulent AT&T wireless account to be opened utilizing the PII of victim A.S.

b. Immediately after creating the fraudulent A.S. AT&T account, co-conspirators purchased two BlackBerry Torch smartphones using a Visa credit card ending in 7438 stolen from victim J.H.

c. A co-conspirator caused the two BlackBerry Torch smartphones to be

shipped to the home of victim C.J. in Burlington, IA.

d. On or about March 5, 2012, defendant **AYELOTAN** sent an email to defendant **SHONEKAN**, with the subject line "POST OFFICE LABEL TRACY", for the purpose of having defendant **SHONEKAN** obtain and send fraudulently purchased United States Postal Service click and ship labels to victim C.J. and defendant **HLUNGWANE** for the two BlackBerry Torch smartphones.

e. Between on or about March 5, 2012 and March 6, 2012, defendant **SHONEKAN** emailed fraudulently purchased United States Postal Service shipping labels utilizing the stolen credit card ending in 7624 belonging to victim L.D. for shipment of the two BlackBerry Torch smartphones.

f. On or about March 6, 2012, defendant **AYELOTAN** sent an email to defendant **OYELADE** which contained multiple shipping labels purchased from the United States Postal Service with a compromised credit card ending in 7264 owned by victim L.D. These shipping labels were used to re-ship the BlackBerry Torch smartphones from Burlington, IA to Pretoria, South Africa.

g. On or about March 6, 2012, defendant **OYELADE** forwarded the email with the shipping labels to C.J. along with instructions to C.J. on how to re-ship the fraudulently obtained smartphones to Pretoria, South Africa.

h. On or about March 6, 2012, C.J. shipped the fraudulently obtained smartphones via the United States Postal Service to defendant **HLUNGWANE,** in Pretoria, South Africa.

84. The following acts in furtherance relate to the interstate shipping of merchandise obtained with the stolen PII and the compromised credit and bank accounts of victims M.H. and M.P.

a. On or about April 6, 2012, co-conspirators caused a fraudulent AT&T

wireless account to be opened utilizing the PII of victim M.H.

b. Immediately after creating the fraudulent M.H. AT&T wireless account, co-conspirators purchased two BlackBerry Torch smartphones utilizing a Visa credit card ending in 8536 stolen from victim M.P.

c. A co-conspirator caused the two BlackBerry smartphones to be shipped to the home of victim J.B. in Collins, Mississippi.

d. On or about April 12, 2012, defendant **LAWANI** sent an email with a United States Postal Service shipping label to J.B. The postal label was purchased through the United States Post Office click and ship service using the stolen credit card of an unknown victim. This email contained instructions to J.B. on how to re-ship the fraudulently obtained smartphones to Pretoria, South Africa.

e. Between April 12 and 16 2012, J.B. shipped the fraudulently obtained smartphones via the United States Postal Service to an address in Pretoria, South Africa.

85. The following acts in furtherance relate to the interstate shipping of merchandise obtained with the stolen PII and the compromised credit and bank accounts of victims S.L. and B.D.

a. On or about September 10, 2013, co-conspirators caused a fraudulent AT&T wireless account to be opened utilizing the PII of victim S.L.

b. Immediately after creating the fraudulent S.L. AT&T wireless account, co-conspirators purchased two BlackBerry Torch smartphones utilizing a Discover credit card ending in 4273 stolen from victim B.D.

c. A co-conspirator caused the two BlackBerry smartphones to be shipped to the home of victim J.D. in Lewisburg, PA.

d. On or about September 13, 2013, defendant **AYELOTAN** sent an email to defendant **RAHEEM** which contained multiple shipping labels purchased from the United States Postal Service with a compromised credit card. These shipping labels were used to re-ship the

BlackBerry smartphones to defendant **HLUNGWANE** in Pretoria, South Africa.

e. On or about September 16, 2013, the fraudulent AT&T wireless account in the name of S.L. was used to purchase two additional smartphones, a Samsung Galaxy and a Nokia Lumina. These smartphones were also shipped to J.D. in Lewisburg, PA.

f. On or about September 19, 2013, defendant **AYELOTAN** sent an email to defendant **RAHEEM** which contained multiple shipping labels purchased from the United States Postal Service with a compromised credit card. These shipping labels were used to re-ship the Samsung and Nokia smartphones to defendant **HLUNGWANE** in Pretoria, South Africa.

g. On or about October 2, 2013, a South Africa law enforcement officer purchased from defendant **HLUNGWANE** one of the BlackBerry smartphones obtained through the fraudulent AT&T wireless account in the name of S.L.

86. The following acts in furtherance relate to the interstate shipping of merchandise obtained with the stolen PII and the compromised credit and bank accounts of victims H.Q., H.S. and an unknown victim.

a. On or about September 23, 2013, co-conspirators caused a fraudulent AT&T wireless account to be opened utilizing the PII of victim H.Q.

b. After creating the fraudulent H.Q. AT&T wireless account, co-conspirators purchased two smartphones utilizing an American Express credit card ending in 1002 stolen from an unknown victim and a Visa card ending in 3204 stolen from H.S.

c. A co-conspirator caused the two smartphones to be shipped to the home of victim D.W. in Liberty Lake, WA.

d. Between on or about September 24, 2013 and October 2, 2013, the defendants, **AYELOTAN** and **RAHEEM,** corresponded via Yahoo! Messenger regarding the receipt and shipment of the fraudulently obtained smartphones.

e. On or about October 2, 2013, defendant **AYELOTAN** sent an email to

defendant **RAHEEM** which had attached to it a United States Postal Service shipping label that had been obtained with a compromised credit card. This shipping label was used by D.W. to re-ship the fraudulently obtained smartphones to defendant **AYELOTAN** in Pretoria, South Africa.

f. On or about October 25, 2013, a South Africa law enforcement officer purchased one of the smartphones purchased through the fraudulent AT&T wireless account in the name of H.Q. from defendant **HLUNGWANE.**

87. The following acts in furtherance relate to the interstate shipping of merchandise obtained with the Discover credit card ending in 9194 of victim J.G.

a. On or about March 14, 2013, defendant **MEWASE** sent an email to defendant **FARIN** with the subject line "LABEL DONE." Attached to the email were United States Postal Service click and ship labels purchased with the compromised Discover credit card ending in 9194 of victim J.G.

b. On or about March 14, 2013, defendant **FARIN** sent an email to defendant **OMORAKA** with the subject line "TX LABEL DONE" containing the fraudulently purchased postal labels previously sent by defendant **MEWASE**.

c. On or about March 14, 2013, defendant **OMORAKA** forwarded the email, subject line "TX LABEL DONE", to victim B.B. for shipment of two cameras to "Alexander Femi" in Pretoria, South Africa.

88. The following acts in furtherance relate to the interstate shipping of merchandise obtained with the stolen identity and credit card account of victim A.S.

a. On or about August 2, 2011, defendant **ODEBUNMI** sent an email to defendant **FARIN** with the subject line "Labels Needed for 2 Boxes From HUNTER" and containing in the narrative portion as the Sender's name and address victim M.M. in Fayette, Mississippi.

b. On or about August 2, 2011, defendant **FARIN** emailed defendant

ODEBUNMI with the subject line "DONE." Attached to the email were two Federal Express international shipping labels 3503 and 3937. Label 3503 was purchased through the stolen identity and credit card account ending in 3690 of victim A.S.

c. On or about August 3, 2011, defendant **ODEBUNMI** emailed defendant **ADEGBEMIGUN** with the subject line "LABELS FROM HUNTER." Attached to the email were the FedEx international shipping labels Tracking numbers ending in 3502 and 3937.

d. On or about August 3, 2011, defendant **ADEGBEMIGUN** emailed victim M.M. with the subject line "THE LABELS." The narrative portion of the email states: "My Love here is the lebel They might come to your house today and pick it up around 3 to 4pm, Or you can go and drop it off there. I think that will be better, I love you my angel." Attached to the email were the FedEx international shipping labels Tracking numbers ending in 3502 and 3937.

89. The following acts in furtherance relate to the Discover credit card account ending in 4163 belonging to victim V.S.

a. On or about January 15, 2013, the Discover credit card account belonging to V.S. was stolen by unknown co-conspirators and shared with other co-conspirators.

b. Between on or about January 15, 2013 and on or about February 6, 2013, V.S.'s Discover credit card was used to fund a pre-paid American Express SERVE debit card account held in the name dbienstock@ymail.com. During this time period, approximately $500 was charged to the compromised Discover credit card of V.S. for this purpose.

c. On or about January 15, 2013, defendant **AYELOTAN** was a party to an email that contained the PII of multiple individuals including credit card information. The email referred to the email address dbienstock@ymail.com. On January 16, 2013, defendant **AYELOTAN** was a party to an email with the address eric_familyphysician@dr.com.

d. On or about January 16, 2013, co-conspirators caused the SERVE account and peer to peer account held in the name of dbienstock@ymail.com to make a peer-to-peer funds

transfer of $100 to the SERVE account in the name of eric_familyphysician@dr.com.

e. On or about January 16, 2013, co-conspirators caused the SERVE account in the name of eric_familyphysician@dr.com to make a peer-to-peer funds transfer of $500 to the SERVE account in the name of leslie.duncan49@yahoo.com.

f. On or about January 16, 2013, the defendants, **RAHEEM and AYELOTAN,** corresponded via Yahoo! Messenger regarding the loading of the SERVE debit account held in the name of "leslie."

g. On or about January 17, 2013, $500 was withdrawn from an ATM in Shelby, North Carolina using the debit card associated with the leslie.duncan49@yahoo.com SERVE account.

h. On or about January 17, 2013, L.D. wire transferred $420 to defendant **HLUNGWANE** via a Western Union agent located in Shelby, North Carolina.

i. On or about January 17, 2013, defendant **RAHEEM** received an email from leslie.duncan49@yahoo.com, which contained wire transaction number and the amount of $420.

90. The following acts in furtherance relate to the compromise of the credit card accounts of victims M.M. ending in 6274, S.S. ending in 7993, L.D. ending in 1264, R.M. ending in 6686 and D.J. ending in 6288.

a. On or about December 16 and 17, 2012, co-conspirators used the respective credit card accounts of M.M., S.S. and L.D. to fund $100 to each of three AmEx SERVE pre-paid accounts held in the names of getupfromhere@yahoo.com, nikefindswer22@yahoo.com, and messiyou23@yahoo.com.

b. On or about December 16 and 17, 2102, three SERVE accounts, respectively held in the names of getupfromhere@yahoo.com, nikefindswer22@yahoo.com, and messiyou23@yahoo.com, each engaged in peer-to-peer transfers, sending approximately $250 in the aggregate to a SERVE account held in the name of mailmenow546@yahoo.com.

c. On or about December 18, 2012, the respective credit card accounts of R.M. and D.J. were fraudulently used to fund a total of $200 to a SERVE account held in the name of muyulakings33@yahoo.com.

d. On or about December 18, 2012, the SERVE account held in the name of mailmenow546@yahoo.com received a peer-to-peer transfer of $200 from the SERVE account held in the name of muyulakings33@yahoo.com.

e. On or about December 12, 2012, defendant **ODEBUNMI** was a party to an email that contained approximately 82 email accounts that were to be used to create American Express SERVE accounts. The email addresses getupfromhere@yahoo.com, nikefindswer22@yahoo.com, messiyou23@yahoo.com and muyulakings33@yahoo.com were included in this email.

f. On or about December 18, 2012, the SERVE account held in the name of mailmenow546@yahoo.com conducted a peer-to-peer transfer of $495 to a SERVE account held in the name of flammingshadows17@yahoo.com.

g. On or about December 10, 2012, defendant **ODEBUNMI** received an email from an unknown co-conspirator that contained the email address and the answers to two challenge questions for the associated SERVE account.

h. On or about December 19, 2012, $483 was withdrawn from an ATM in Carthage, Mississippi, using the debit card associated with the flammingshadows17@yahoo.com SERVE account.

i. On or about December 19, 2012, an individual known as L.E. wire transferred $470 to an individual known as N.B. in Pretoria, South Africa, from a Wal-Mart located in Carthage, Mississippi.

91. The following acts in furtherance relate to the compromise of the credit card accounts of victims J.M. ending in 2067, R.M. ending in 2543, D.F. ending in 5710, J.M. ending in

8685, and unknown card ending in 6714.

a. From on or about January 19, 2013 through on or about January 22, 2013, the respective credit card accounts of J.M., R.M., D.F., J.M. and unknown were used to fraudulently fund approximately $500 in total to AmEx SERVE pre-paid accounts held in the names garnettry82@yahoo.com, stephentrezza@yahoo.com, larry.anthony55@yahoo.com, glennsattelberg1961@gmail.com and elissagoffm@yahoo.com.

b. On or about January 23, 2013, the SERVE account held in the name garnettry82@yahoo.com conducted a peer-to-peer transfer of $50 to a SERVE account held in the name of larry.anthony55@yahoo.com.

c. On or about January 23, 2013, the SERVE account held in the name stephentrezza@yahoo.com conducted a peer-to-peer transfer of $100 to a SERVE account held in the name of glennsattelberg1961@gmail.com.

d. On or about January 23, 2013, the SERVE account held in the name elissagoffm@yahoo.com conducted a peer-to-peer transfer of $150 to a SERVE account held in the name of glennsattelberg1961@gmail.com.

e. On or about January 23, 2013, the SERVE account held in the name larry.anthony55@yahoo.com conducted a peer-to-peer transfer of $200 to a SERVE account held in the name of glennsattelberg1961@gmail.com.

f. On or about January 23, 2013, the SERVE account held in the name glennsattelberg1961@gmail.com conducted a peer-to-peer transfer of $500 to a SERVE account held in the name of michaelophthalmology@yahoo.com.

g. On or about January 22, 2013, defendants **AYELOTAN** and **FARFAN** exchanged emails wherein defendant **FARFAN** provided the card number, security code and the expiration date of a debit card associated with a SERVE account held in the name michaelophthalmology@yahoo.com to defendant **AYELOTAN.**

h. On or about January 23, 2013, defendant **AYELOTAN** sent an email to defendant **FARFAN** which contained the login information for the SERVE account held in the name michaelophthalmology@yahoo.com.

i. On or about January 23, 2013, defendants **AYELOTAN** and **FARFAN** exchanged emails wherein defendant **AYELOTAN** instructs defendant **FARFAN** to use a card to withdraw $500 from an ATM, and to keep $150 herself and to wire transfer the remainder of the funds via Western Union or Money Gram to defendant **HLUNGWANE** in Pretoria, South Africa.

j. On or about January 25, 2013, three separate withdrawals were made from an ATM in Lynnwood, California using the debit card associated with the michaelophthalmology@yahoo.com SERVE account. The withdrawals were in the amounts of $202.75, $202.75 and $82.75 respectively. The ATM used to make the withdrawals was located approximately one mile from the residence of defendant **FARFAN.**

k. On or about January 25, 2013, defendant **FARFAN** sent an email to defendant **AYELOTAN** wherein defendant **FARFAN** explains that she has wire transferred $300 to defendant **HLUNGWANE** in Pretoria, South Africa.

All in violation of Section 1349, Title 18, United States Code.

COUNT 2

92. That from on or about November 2001, and continuing until on or about the date of the indictment, in Harrison County in the Southern Division of the Southern District of Mississippi, and elsewhere, the defendants, **OLADIMEJI SEUN AYELOTAN, TESLIM OLAREWAJU KIRIJI, RASAQ ADEROJU RAHEEM, DENNIS BRIAN LADDEN, ADEKUNLE ADEFILA, RHULANE FIONAH HLUNGWANE, OLASUPO MOFOLUWASHO ODEBUNMI, GENOVEVA FARFAN, GABRIEL OLUDARE ADENIRAN, SUSAN ANN VILLENEUVE, OLUSEGUN SEYI SHONEKAN, TAOFEEQ OLAMILEKAN OYELADE, ODUNTAN SIKIRU LAWANI, SESAN OLUMIDE FARIN, OLUFEMI OBARO**

OMORAKA, FEMI ALEXANDER MEWASE, and ANUOLUWAPO SEGUN ADEGBEMIGUN, did knowing and willfully conspire with each other and with others known and unknown to the Grand Jury, to commit offenses against the United States as follows:

93. a. Identity Theft as prohibited by Section 1028(a)(7), Title 18, United States Code, that is the possession, transfer and use in or affecting interstate or foreign commerce, without lawful authority, the means of identification of another person with the intent to commit, or to aid or abet or in connection with unlawful activities that constitute violations of Federal law, or that constitute felonies under State or local law;

b. Use of unauthorized access devices as prohibited by Section 1029(a)(3), Title 18, United States Code, that is knowingly and with intent to defraud traffic in or use fifteen or more unauthorized access devices;

c. Use of unauthorized access devices as prohibited by Section 1029(a)(5), Title 18, United States Code, that is knowingly and with intent to defraud effects transactions with 1 or more access devices issued to another person or persons to receive payment or other thing of value aggregating $1000 or more during any 1-year period;

d. Theft of government funds as prohibited by Section 641, Title 18, United States Code in that to embezzle, steal, purloin and knowingly convert to their own use or the use of another, in excess of $1000 in money or thing of value of the United States of America and the United States Postal Service (hereinafter U.S.P.S.), a department or agency of the United States of America.

94. It was a part of the conspiracy that the defendants would obtain personal identifying information (PII), credit card and bank data from international hackers and use that information to obtain, use and traffic in unauthorized credit cards; take over financial accounts; use fraudulently obtained credit card data to steal government funds by fraudulently purchasing online U.S.P.S. shipping labels; and obtain, transfer, possess and use the unauthorized PII as a means of identification to commit violations of federal and state law.

95. In furtherance of the conspiracy and to carry out its objectives, the overt acts in paragraphs 1 through 91 are re-alleged and incorporated as if set forth herein.

96. The following acts in furtherance relate to the unauthorized use of a credit card in interstate or foreign commerce and obtained more than $1,000 in a one-year period.

a. On or about August 2, 2011, defendant **ODEBUNMI** sent an email to defendant **FARIN** with the subject line "Labels Needed For 2 Boxes From HUNTER."

b. On August, 2011, defendant **FARIN** emailed defendant **ODEBUNMI** with the subject line "Done." Attached to the email were Federal Express shipping labels ending in tracking numbers 3503 and 3937 purchased with the use of an unauthorized American Express credit card belonging to victim A.S. The labels reflected the sender as M.M. a resident of the Southern District of Mississippi with the recipients as defendants **ODEBUNMI** and **ADEGBEMIGUN**.

c. On August 3, 2011, defendant **ADEGBEMIGUN** sent an email to M.M. with the subject line "THE LABELS." Attached to the email were Federal Express shipping labels ending in 3503 and 3937.

d. On August 3, 2011, the defendants caused a package with a label ending in 3503 to be deposited with Federal Express for delivery in South Africa and with delivery charges of $1,656.15.

e. On August 12, 2011, the defendants caused a package with a label ending in 3937 to be deposited with Federal Express for delivery to South Africa and with delivery charges of $975.05.

All in violation of Section 371, Title, 18 United States Code.

COUNTS 3-8

97. In furtherance of the scheme and artifice to defraud and to carry out its objectives, the allegations in paragraphs 1-91 are re-alleged and incorporated as if set forth herein.

98. Beginning in at least 2001, and continuing until the date of this indictment, in Harrison County, in the Southern Division of the Southern District of Mississippi, and elsewhere, the defendants, **OLADIMEJI SEUN AYELOTAN, RASAQ ADEROJU RAHEEM, DENNIS BRIAN LADDEN RHULANE FIONAH HLUNGWANE, OLUSEGUN SEYI SHONEKAN, TAOFEEQ OLAMILEKAN OYELADE, and ODUNTAN SIKIRU LAWANI**, aided and abetted by each other and with others known and unknown to the grand jury, did knowingly devise and intend to devise a scheme and artifice to defraud and to obtain money or property by means of false and fraudulent pretenses and representations, and for the purpose of executing and attempting to execute the scheme, knowingly and unlawfully causing to be delivered by the United States Postal Service and private and commercial interstate and foreign carriers matters according to the directions thereon, on or about the dates set forth below, by the United States Postal Service and Federal Express, to the persons/entities whose names and cities of residence are listed below, each constituting a separate count herein:

Count	Date	Description	Addressee
3	9/26/2011	2 BlackBerry Torch smartphones	N.J. Biloxi, MS
4	12/14/2011	Commerce Bank check $3,000	N.J. Biloxi, MS
5	4/6/2012	2 BlackBerry Torch smartphones	J.B. Collins, MS
6	4/16/2012	2 BlackBerry Torch smartphones	Pretoria, South Africa

7	10/29/2012	Capitol One Bank check $5,400	N.J. Biloxi, MS
8	9/9/2012	Regions Bank check $3,550	C.B. Lucedale, MS

All in violation of Sections 1341 and 2, Title 18, United States Code.

NOTICE OF INTENT TO SEEK CRIMINAL FORFEITURE

As a result of committing the offenses alleged in this Indictment, the defendants shall forfeit to the United States all property involved in or traceable to property involved in the offenses, including but not limited to all proceeds obtained directly or indirectly from the offenses, and all property used to facilitate the offenses. Further, if any property described above, as a result of any act or omission of the defendants: (a) cannot be located upon the exercise of due diligence; (b) has been transferred or sold to, or deposited with, a third party; (c) has been placed beyond the jurisdiction of the Court; (d) has been substantially diminished in value; or (e) has been commingled with other property, which cannot be divided without difficulty, then it is the intent of the United

States to seek a judgment of forfeiture of any other property of the defendants, up to the value of the property described in this notice or any bill of particulars supporting it.

All pursuant to Section 981(a)(1)(C), Title 18, United States Code and Section 2461, Title 28, United States Code.

GREGORY K. DAVIS
United States Attorney

A TRUE BILL:

Foreperson of the Grand Jury

This indictment was returned in open court by the foreperson or deputy foreperson of the grand jury on this the 9th day of April, 2014.

UNITED STATES MAGISTRATE JUDGE

A TRUE COPY, I HEREBY CERTIFY.
ARTHUR JOHNSTON, CLERK
BY:
DEPUTY CLERK