UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

UNITED STATES OF AMERICA	)	
	)	
v.	)	
	)	
HIEU MINH NGO,	)	1:12-cr- 144-01/02-PB
a/k/a "hieupc," and	)	
	)	
JOHN DOE ONE,	)	
a/k/a "rr2518" and "Wan Bai"	)	

_____

INDICTMENT

The Grand Jury charges:

Introduction

At all times material to this Indictment

1. Defendant HIEU MINH NGO ("NGO"), also known by online monikers that include "hieupc" and "traztaz659," resided in New Zealand and Vietnam. He is one of the control persons and administrators for the websites "findget.me" and "superget.info," and its associated data.
2. JOHN DOE ONE, also known by online monikers that include "rr2518" and "Wan Bai," resided in an unknown location. He is one of the control persons and administrators for the website "findget.me," and its associated data.
3. Personally identifiable information ("PII") can include individuals' names, addresses, social security numbers, dates of birth, places of work, duration of work, state driver's license numbers, mothers' maiden names, bank account numbers, bank routing numbers, e-mail account names, and other account passwords.

4. "Payment card data" refers to credit, debit, and/or gift card numbers and associated data that can be used to make charges on an account. The data typically includes the payment card number, expiration date, Card Verification Value ("CVV") number, account holder name, account holder address, and phone number.

5. "Carding" refers to an assortment of illegal activities revolving around the theft and fraudulent use of PII and payment card data, and "carders" refers to individuals who are engaged in illegal carding activity.

6. "Carder forums" are websites that provide an online marketplace for various carding activities. Typically, membership is required. Members can purchase a variety of types of goods and services, including other individuals' PII and payment card data. The members typically communicate via email messages, private messages, or via posts to the forum.

7. "Fulls" or "fullz" ("Full Info(s)") is a slang term that carders use to describe a package of PII. The defendants and their co-conspirators acquired and offered for sale "fullz" that typically included the following types of PII: names, addresses, social security numbers, dates of birth, places of work, duration of work, state driver's license numbers, mothers' maiden names, bank account numbers, bank routing numbers, e-mail account names, and other account passwords.

8. "Fullz" are frequently used by carders to take over the identity of a person in order to engage in various types of fraudulent activities, without the identity theft victim's consent. These can include opening new financial accounts in the victim's name and making fraudulent purchases on, or transfers of funds from, those accounts; taking out loans in the victim's name; and filing fraudulent tax refund requests with the IRS on behalf of the victim.

9. "Liberty Reserve" ("LR") is an anonymous, offshore, electronic currency system that enables individuals with LR accounts to transfer money through offshore accounts to other LR

account holders worldwide. Transactions can be made anonymously, and the only form of identification that LR requires to create an account is an e-mail address.

10. From 2007-2012, the defendants, and other members of the conspiracy, acquired, offered for sale, sold, and/or transferred to others "fullz" of more than 500,000 individuals. They repeatedly acquired and transferred to others "fullz" of individuals located in the District of New Hampshire. The bank account information contained in those "fullz" included bank branches located in the District of New Hampshire. Furthermore, they repeatedly sold and transferred "fullz" to one or more buyers located in the District of New Hampshire.

11. From 2007-2012, the defendants, and other members of the conspiracy, acquired, offered for sale, sold, and/or transferred to others, stolen payment card data. The stolen payment card data typically included the victim account holder's payment card number, expiration date, CVV number, account holder name, account holder address, and phone number. They repeatedly acquired and transferred to others stolen payment card data for account holders located in the District of New Hampshire.

COUNT ONE

Conspiracy to Commit Wire Fraud
(18 U.S.C. §§ 1343 & 1349)

12. The allegations set forth in paragraphs 1 through 11 of the Indictment are re-alleged and incorporated as set forth herein.

13. Beginning at a date uncertain, but at least as early as 2007, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, but at least as late as June 2012, in the District of New Hampshire and elsewhere, the defendants

HIEU MINH NGO
and
JOHN DOE ONE

knowingly and intentionally attempted and combined, conspired, and agreed with each other, and with other persons known and unknown to the Grand Jury, to devise a scheme and artifice to defraud others, namely, merchants, financial institutions, and account holders, and to obtain money and property, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme and artifice to defraud, did transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Sections 1343 and 1349.

Objects of the Conspiracy

14. It was the object of the conspiracy for the defendants and their co-conspirators to acquire, offer for sale, sell, and transfer to others, “fullz,” including “fullz” of individuals residing in New Hampshire, which information was to be used to engage in various types of fraudulent carding activities, including but not limited to opening financial and payment card accounts in these individuals’ names and making fraudulent charges on, or transfers of funds from, those accounts.

15. It was further the object of the conspiracy for the defendants and their co-conspirators to acquire, offer for sale, sell, and transfer to others, stolen payment card data, including payment card data of individuals residing in New Hampshire, which information was to be used to engage in various types of fraudulent carding activities, including but not limited to making fraudulent charges on, or transfers of funds from, those accounts.

Manner and Means of the Conspiracies

16. It was part of the conspiracy that the defendants and their co-conspirators acquired payment card data of individuals, including individuals located in the District of New Hampshire.

17. It was further part of the conspiracy that the defendants and their co-conspirators acquired "fullz" of over 500,000 individuals, including individuals located in the District of New Hampshire.

18. It was further part of the conspiracy that the defendants and their co-conspirators operated one or more carder forums, including "superget.info" and "findget.me," where they stored and offered for sale "fullz" and other PII, including "fullz" of individuals located in the District of New Hampshire.

19. On their "superget.info" and "findget.me" carder forums, the defendants and their co-conspirators offered buyers the option either to obtain a specified quantity of "fullz" or to submit a "query" of a particular name in order to obtain that person's associated PII, including the person's date of birth and social security number. As to the "fullz," the defendants and their co-conspirators offered several categories of PII, depending on how "fresh" the data was (i.e., how recently the data had been acquired). The defendants and their co-conspirators typically charged higher prices for "fullz" that were "fresher" or acquired more recently.

20. It was further part of the conspiracy that the defendants had arrangements with "re-sellers," including re-sellers who used the online monikers "attackervietnam" and "ssndob.sll." The

defendants charged a fee to these re-sellers, and in exchange, the re-seller could access and re-sell the defendants' stolen payment card data, "fullz," and other PII.

21. It was further part of the conspiracy that the defendants and their co-conspirators created one or more accounts with "Liberty Reserve" ("LR") and used those accounts to receive funds for the stolen payment card data, "fullz," and other PII that they sold. They instructed purchasers to create their own LR accounts in order to pay for the stolen payment card data, "fullz," and other PII. The defendants and their co-conspirators provided their LR account information to purchasers and instructed purchasers to transfer the required funds from the purchasers' LR accounts into the defendants' LR accounts.

22. It was further part of the conspiracy that the defendants and their co-conspirators opened various e-mail accounts, including "hieupc@gmail.com," "traztaz659@gmail.com," and "rr2518@gmail.com," and used those accounts to communicate with one another, to communicate with prospective and actual buyers and sellers, and to transfer stolen payment card data, "fullz," and other PII.

23. It was further part of the conspiracy that the defendants and their co-conspirators, typically using these e-mail accounts, electronically transferred stolen payment card data, including payment card data belonging to individuals located in New Hampshire, to others.

24. It was further part of the conspiracy that the defendants and their co-conspirators, typically using these e-mail accounts, electronically transferred stolen "fullz," including "fullz" of individuals located in New Hampshire, to other buyers, including to one or more buyers located in the District of New Hampshire.

Overt Acts

25. In furtherance of the conspiracy, and to effect and accomplish the objects of it, one or more of the defendants or conspirators, both indicted and unindicted, committed, among others, the following overt acts in the District of New Hampshire and elsewhere:

Setting Up Carding Web Sites, E-mail Accounts, and Liberty Reserve Accounts

26. On or about July 3, 2010, NGO registered the domain name "superget.info" with Domains by Proxy LLC, a webhosting company and registrar with computer servers located in Arizona.

27. On or about December 14, 2010, NGO subscribed for a webhosting account with VPS.net and obtained "cloud hosting" services from VPS.net for purposes of storing large amounts of electronic data. NGO continued to pay the monthly fee at least through October 2012. VPS.net is a webhosting company based in Utah with computer servers located in Illinois.

28. On or about November 18, 2011, NGO registered the domain name "findget.me" with Domains by Proxy LLC, located in Arizona.

29. On or about May 18, 2010, NGO created an e-mail account with Google for the account name "traztaz659@gmail.com." In the account subscriber records, NGO identified "Traci Donnell" as the subscriber.

30. On or about March 10, 2009, JOHN DOE ONE created an e-mail account with Google, for the account name "rr2518@gmail.com."

31. In or before January 2010, NGO opened a Liberty Reserve account for use in buying and selling payment card data, "fullz," and other PII.

32. In or before November 2011, JOHN DOE ONE opened a Liberty Reserve account, using the name "Traci Donnell," which NGO had identified as the subscriber in opening the traztaz659 Gmail account, for use in buying and selling payment card data, "fullz," and other PII.

Storing Stolen PII

33. On or before December 2011, members of the conspiracy stored "fullz" for over 500,000 individuals on their "findget.me" website. These included "fullz" of one or more individuals located in the District of New Hampshire.

Transferring New Hampshire Residents' "Fullz" and Stolen Payment Card Data

34. On or about November 29, 2007, NGO, using the e-mail account "hieupc@gmail.com," sent an email message to "attackervietnam@gmail.com" that contained stolen payment card data for approximately 300 individuals (including payment card numbers, expiration date, CVV number, account holder names, account holder address), as well as what appears to be the account holder's Internet Protocol ("IP") address, at least three of whom are New Hampshire residents.

35. On or about November 30, 2007, NGO, using the "hieupc" e-mail account, sent an email message to "attackervietnam@gmail.com" that contained stolen payment card data for approximately 200 individuals (including payment card numbers, expiration date, CVV number, account holder names, account holder address), as well as what appears to be the IP address, at least two of whom are New Hampshire residents.

36. On or about December 8, 2007, NGO, using the "hieupc" e-mail account, sent an email message to "attackervietnam@gmail.com" that contained stolen payment card data for approximately 300 individuals, as well as what appears to be the account holder's IP address, at least four of whom are New Hampshire residents.

37. On or about October 2, 2009, NGO, using the "hieupc" e-mail account sent an email message to "kien.info@yahoo.com" that contained stolen payment card data for approximately 117 individuals, as well as what appears to be the account holder's mailing address, email address, at least one of whom is a New Hampshire resident.

38. On or about January 15, 2010, NGO, using the "hieupc" e-mail account, sent an email message to "mrhtseo@gmail.com" that contained stolen payment card data for approximately 72 individuals, as well as what appears to be the account holder's mailing address and phone number, at least one of whom is a New Hampshire resident.

39. On or about June 2, 2011, NGO, using the "hieupc" e-mail account, sent an e-mail message to "ssndob.sll@gmail.com" that contained "fullz" of approximately 660 New Hampshire residents.

40. On or about September 21, 2011, NGO, using the e-mail account "traztaz659@gmail.com," sent an e-mail to "ibu2015@yahoo.com" that contained "fullz" for approximately 31 people, including at least one New Hampshire resident.

41. On or about September 26, 2011, NGO, using the "traztaz659" e-mail account, sent an e-mail to "cafenaumk@gmail.com" that contained "fullz" for approximately 2,160 people, including at least nine New Hampshire residents.

42. On or about September 29, 2011, NGO, using the "traztaz659" e-mail account, sent an e-mail to "cafenaumk@gmail.com" that contained "fullz" for approximately 2,600 people, including at least five New Hampshire residents.

43. On or about November 18, 2011, DOE ONE, using the e-mail account "rr2518," sent an e-mail to "ssndob.sll@gmail.com" stating, "Hi mate! It's still normal for everything. $4600 for 4000 credits and $500 for server fee. Please pay to our LR: U8109093 (Traci Donell) Thanks u."

44. On November 19, 2011, DOE ONE, using the e-mail account "rr2518," forwarded to NGO, at "hieupc@gmail.com," an email from "ssndob.sll@gmail.com," which appeared to be written in Vietnamese, and asked, "I don't know what he wrote, can you help me?" NGO later sent an e-mail directly to "ssndob.sll," explained that DOE ONE does not understand Vietnamese, and offered to translate into English.

45. On November 26, 2011, DOE ONE, using the e-mail account "rr2518," sent an email to 13 email addresses with the subject line "hi guy (admin of findget.me)," stating, "Hi, I see you as a big customer at findget.me. If you want to have a big deal with us, please let us know. Currently we have some big plans for users like you" $5000 for 22,000 credits. $10,000 for

50,000 credits. (with fully 24/24 hours support from admin if you have any issues. Thank you."

46. On December 2, 2011, NGO, using the "traztaz659" e-mail account, sent an e-mail to "cafenaumk@gmail.com" that contained "fullz" for approximately 270 people.

47. On December 15, 2011, DOE ONE, using the e-mail account "rr2518," sent an e-mail to "kendyphongzz@yahoo.com" that contained "fullz" of approximately 420 individuals.

48. On December 23, 2011, DOE ONE, using the e-mail account "rr2518," sent an email to "kendyphongzz" that contained "fullz" of approximately 200 individuals.

49. On December 27, 2011, DOE ONE, using the e-mail account "rr2518," sent an email to "kendyphongzz" that contained "fullz" of approximately 105 individuals.

50. On December 19, 2011, DOE ONE, using the e-mail account "rr2518," sent an email to "gregory.payne08@gmail.com" that contained "fullz" of approximately 520 individuals.

51. On January 9, 2012, DOE ONE, using the e-mail account "rr2518," sent an email to "barrylevin85@yahoo.com" that contained "fullz" of approximately 220 individuals.

52. On the same date, DOE ONE, using the e-mail account "rr2518," sent an email to "dieterhellstorm@yahoo.com" that contained "fullz" of approximately 20 individuals' PII.

53. On January 10, 2012, DOE ONE, using the e-mail account "rr2518," sent an email to "cafenaumk@gmail.com" that contained "fullz" of approximately 270 individuals.

54. On January 24, 2012, DOE ONE, using the e-mail account "rr2518," sent an email to "mprk02@yahoo.co.uk" that contained "fullz" of approximately 22 individuals.

Offering to Sell Stolen PII to Undercover Agent in New Hampshire

55. In or about November 2011, members of the conspiracy, on their carder forum "findget.me," instructed a visitor to that forum to send an e-mail message to "rr2518@gmail.com" in order to open an account with "findget.me." Unbeknownst to the defendants, the visitor was an undercover agent located in New Hampshire ("UC agent"). They also instructed that UC

agent to open an account with "Liberty Reserve" in order to engage in any financial transactions with them.

56. On or about November 21, 2011, DOE ONE sent an e-mail message to the UC agent with a username and password for him to use in order to open an account with findget.me, and created an account on "findget.me" on behalf of the UC agent.

57. From in or about November 29, 2011, through in or about June 2012, DOE ONE, using the e-mail account "rr2518," engaged in a series of e-mail communications with the UC agent in which they discussed the UC agent's interest in purchasing "fullz."

Transferring "Fullz" to Undercover Agent in New Hampshire

58. On or about November 29, 2011, after the UC agent purchased "fullz" from "rr2518" using Liberty Reserve, DOE ONE sent an e-mail message to the UC agent that contained "fullz" of approximately 245 individuals and included New Hampshire residents.

59. Also on or about November 29, 2011, after the UC agent purchased "fullz" from "rr2518" using Liberty Reserve, DOE ONE sent an e-mail message to the UC agent that contained "fullz" of approximately 50 individuals and included New Hampshire residents.

60. On or about December 5, 2011, after the UC agent purchased "fullz" from "rr2518" using Liberty Reserve, DOE ONE sent an e-mail message to the UC agent that contained "fullz" of approximately 90 individuals and included New Hampshire residents.

61. On or about June 5, 2012, after the UC agent sent an e-mail message to DOE ONE stating that he wanted to "buy some really fresh fullz for New Hampshire males between 18-40 years. The ones I bought before I couldn't open credit cards and almost got caught. J how much for 25? How fresh are they?," DOE ONE sent an e-mail message to the UC agent that responded ".5$ per one info".

In violation of Title 18, United States Code, Sections 1343 & 1349.

COUNTS TWO THROUGH FOUR
Wire Fraud
(18 U.S.C. §§ 1343 & 2)

62. The allegations set forth in paragraphs 1 through 11 and 14 through 61 of the Indictment are re-alleged and incorporated as set forth herein.

63. Beginning at a date uncertain, but at least as early as 2007, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, but at least as late as June 2012, in the District of New Hampshire and elsewhere, the defendants

HIEU MINH NGO
and
JOHN DOE ONE

devised and intended to devise, and aided and abetted others in devising, a scheme and artifice to defraud, and for obtaining money and property by means of materially false and fraudulent pretenses, representations, and promises, as described in Paragraphs 14 and 15 above.

64. In furtherance of, and for the purpose of executing, such scheme and artifice to defraud, in the District of New Hampshire and elsewhere, the defendants

HIEU MINH NGO
and
JOHN DOE ONE

transmitted and caused to be transmitted by means of wire communication, as more particularly described below, in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds.

Count Number	Description of Wire	Location of Wire	Date of Wire
Two	DOE e-mail to New Hampshire UC agent re username and password for findget.me website	Sent to District of New Hampshire	11/21/11
Three	DOE e-mail to New Hampshire UC agent containing 245 "fullz," including for New Hampshire residents	Sent to District of New Hampshire	11/29/11
Four	DOE e-mail to New Hampshire UC agent containing 90 "fullz," including for New Hampshire residents."	Sent to District of New Hampshire	12/5/11

In violation of Title 18, United States Code, Sections 1343 and 2, and Pinkerton v. United States, 328 U.S. 640 (1946).

COUNT FIVE
Conspiracy to Commit Identification Fraud
(18 U.S.C. §§ 1028(f) & 1028(a)(7))

65. The allegations set forth in paragraphs 1 through 11, 14 through 61 and 64 of the Indictment are re-alleged and incorporated as set forth herein.

66. Beginning at a date uncertain, but at least as early as 2007, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, but at least as late as June 2012, in the District of New Hampshire and elsewhere, the defendants

HIEU MINH NGO
and
JOHN DOE ONE

knowingly and intentionally attempted and combined, conspired, and agreed with each other, and with other persons known and unknown to the Grand Jury, to commit an offense under Title 18, United States Code, Section 1028, namely, knowingly transferring possessing, and using, without lawful authority, a means of identification of another person, namely, "fullz" of individuals residing in the District New Hampshire and elsewhere, with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law and that constitutes a felony under applicable State and local law, namely, access device fraud in violation of 18 U.S.C. § 1029(a)(2) and wire fraud in violation of 18 U.S.C. § 1343.

In violation of Title 18, United States Code, Sections 1028(f) and 1028(a)(7), and Pinkerton v. United States, 328 U.S. 640 (1946).

COUNTS SIX THROUGH NINE

Identification Fraud
(18 U.S.C. §§ 1028(a)(7) & 2)

67. The allegations set forth in paragraphs 1 through 11, 14 through 61 and 64 of the Indictment are re-alleged and incorporated as set forth herein.

68. Beginning on or about the dates set forth below, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, in the District of New Hampshire and elsewhere, as set forth below, the defendants

HIEU MINH NGO
and
JOHN DOE ONE

knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, namely, "fullz" of individuals residing in the District of New Hampshire and elsewhere, with the intent to commit, and to aid and abet, and in connection with, unlawful activity that constitutes a violation of Federal law and that constitutes a felony under any applicable State and local law, including: access device fraud, in violation of 18 U.S.C. § 1029(a)(2); aggravated identity theft, in violation of 18 U.S.C. § 1028A; and wire fraud, in violation of 18 U.S.C. § 1343.

Count Number	Information Transferred	Date of Transfer
Six	"Fullz" containing 660 New Hampshire residents' fullz	6/2/11 NGO e-mail to "ssndob.sll@gmail.com"
Seven	"Fullz" containing 9 New Hampshire residents' fullz	9/29/11 NGO e-mail to "cafenaumk@gmail.com"
Eight	"Fullz" of 245, including for New Hampshire residents	11/29/11 DOE e-mail to New Hampshire UC agent
Nine	"Fullz" of 90, including for New Hampshire residents	12/5/11 DOE e-mail to New Hampshire UC agent

In violation of Title 18 United States Code, Sections 1028(a)(7) and 2, and Pinkerton v. United States, 328 U.S. 640 (1946).

COUNTS TEN THROUGH THIRTEEN
Aggravated Identity Theft
(18 U.S.C. §§ 1028A(a)(1) & 2)

69. The allegations set forth in paragraphs 1 through 11, 14 through 61, 64 and 68 of the Indictment are re-alleged and incorporated as set forth herein.

70. Beginning on or about the dates set forth below, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, in the District of New Hampshire and elsewhere, as set forth below, the defendants

HIEU MINH NGO
and
JOHN DOE ONE

knowingly transferred, possessed, and used, without lawful authority, a means of identification of another person, namely, the "fullz" and payment card data of individuals residing in the District New Hampshire and elsewhere, during and in relation to felonies enumerated in 1028A(c), namely, access device fraud in violation of 18 U.S.C. § 1029(a)(2), and wire fraud in violation of 18 U.S.C. § 1343.

Count Number	Information Transferred	Date of Transfer
Ten	"Fullz" containing 660 New Hampshire residents' fullz	6/2/11 Ngo e-mail to "ssndob.sll@gmail.com"
Eleven	"Fullz" containing 9 New Hampshire residents' fullz	9/29/11 Ngo e-mail to "cafenaumk@gmail.com"
Twelve	"Fullz" of 245, including for New Hampshire residents	11/29/11 Doe e-mail to New Hampshire UC agent
Thirteen	"Fullz" of 90, including for New Hampshire residents	12/5/11 Doe e-mail to New Hampshire UC agent

In violation of Title 18, United States Code, Sections 1028A(a)(1) and 2, and Pinkerton v. United States, 328 U.S. 640 (1946).

COUNT FOURTEEN
Conspiracy to Commit Fraud in Connection with Access Devices
(18 U.S.C. §§ 1029(b)(2) & (a)(2))

71. The allegations set forth in paragraphs 1 through 11, 14 through 61, 64, 68 and 70 of the Indictment are re-alleged and incorporated as set forth herein.

72. Beginning at a date uncertain, but at least as early as 2007, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, but at least as late as June 2012, in the District of New Hampshire and elsewhere, the defendants

HIEU MINH NGO
and
JOHN DOE ONE

knowingly and intentionally combined, conspired, and agreed with each other, and with other persons known and unknown to the Grand Jury, to commit an offense under Title 18, United States Code, Section 1029, namely, to knowingly and with intent to defraud traffic in and use one or more unauthorized access devices, namely, "fullz" and payment card data of individuals residing in the District New Hampshire and elsewhere, during any one-year period and by such conduct obtain anything of value aggregating $1,000 or more during that period, said conduct affecting interstate and foreign commerce.

In violation of Title 18, United States Code, Sections 1029(b)(2) and 1029(a)(2), and Pinkerton v. United States, 328 U.S. 640 (1946).

COUNT FIFTEEN

Fraud in Connection with Access Devices
(18 U.S.C. §§ 1029(a)(2) & 2)

73. The allegations set forth in paragraphs1 through 11, 14 through 61, 64, 68 and 70 of the Indictment are re-alleged and incorporated as set forth herein.

74. Beginning on or about the dates set forth below, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, but at least as late as June 2012, in the District of New Hampshire and elsewhere, as set forth below, the defendants

HIEU MINH NGO
and
JOHN DOE ONE

knowingly and with intent to defraud trafficked in and used one or more unauthorized access devices, that is, "fullz" and payment card data of individuals residing in the District New Hampshire and elsewhere, during a one-year period and by such conduct obtained anything of value aggregating $1,000 or more during that period, said conduct affecting interstate and foreign commerce.

In violation of Title 18, United States Code, Sections 1029(a)(2) and 2, and Pinkerton v. United States, 328 U.S. 640 (1946).

November 14, 2012

A TRUE BILL

/s/ Foreperson
Grand Jury Foreperson

JOHN P. KACAVAS
United States Attorney

/s/ Arnold H. Huftalen
Arnold H. Huftalen
Assistant U.S. Attorney

/s/ Mona Sedky
Mona Sedky
Trial Attorney
U.S. Department of Justice