UNITED STATES DISTRICT COURT

FOR THE CENTRAL DISTRICT OF CALIFORNIA

February 2008 Grand Jury

UNITED STATES OF AMERICA, Plaintiff, v. HIEP THANH TRAN, aka John Tran, aka Sam Lam, SORIN ALIN PANAIT, aka "scumpic4u," STEFAN SORIN ILINCA, aka "AzZ," aka "Kahn," aka "Kahnpath," HASSAN PARVEZ, aka "XID," COSTEL BULUGEA, aka "The.Vortex," NICOLAE DRAGOS DRAGHICI, aka Marius Bogdan Natasie, aka "Nonick," DIDI GABRIEL CONSTANTIN, aka "StauLaSoare," aka "Estaulasoare," aka "snoop," FNU LNU, aka "Cryptmaster," FNU LNU, aka "SeleQtor,"	No. CR 08- 08-00584 I N D I C T M E N T [18 U.S.C. § 1962(d): Conspiracy to Violate the Racketeer Influenced and Corrupt Organizations Act; 18 U.S.C. § 1029(b)(2): Conspiracy to Conduct Access Device Fraud; 18 U.S.C. § 1344(2): Bank Fraud; 18 U.S.C. § 1029(a)(1): Production, Use and Trafficking in Counterfeit Access Devices; 18 U.S.C. § 1029(a)(4): Possession of Device-Making Equipment; 18 U.S.C. § 1030(a)(4): Unauthorized Access or Exceeding Authorized Access of a Protected Computer; U.S.C. § 1028A(a)(1): Aggravated Identity Theft; 18 U.S.C. § 1963: Forfeiture; 18 U.S.C. §§ 2(a), (b): Aiding and Abetting and Causing an Act to be Done]

MZ:MA:ma

FLORIN GEORGEL SPIRU,
aka "niggaplease,"
MARIAN DANIEL CIULEAN,
aka "spuickeru,"
IRINEL NICUSOR STANCU,
aka "sicaalex,"
PETRU BOGDAN BELBITA,
aka "CA is SK,"
aka Robert Wilson,
ROLANDO SORIANO,
aka "Loco,"
aka Danny Villalopez,
LEONARD GONZALES,
aka "Bonecrusher,"
NGA NGO,
aka Christina Ngo,
CAROLINE TATH,
SONNY DUC VO,
LOI TAN DANG,
aka Mike,
DUNG PHAN,
THAI HOANG NGUYEN,
ALEX CHUNG LUONG,
FNU LNU,
aka "PaulXSS,"
MIHAI DRAGHICI,
MARIUS SORIN TOMESCU,
aka "Andrei,"
LUCIAN ZAMFIRACHE,
aka Krobelus,
LAURENTIU CRISTIAN BUSCA,
aka "italianu,"
DAN IONESCU,
aka "m1nja,"
OVIDIU-IONUT NICOLA-ROMAN,
MARIUS LNU,
aka "13081981,"
ALEX GABRIEL PARALESCU,
aka "paraiul,"
FNU LNU,
aka "euro_pin_atm,"
and
ANDREEA NICOLETA STANCUTA,
aka "godfather,"

Defendants.

The Grand Jury charges:

GENERAL ALLEGATIONS AND DEFINITIONS

At all times relevant to this indictment, unless otherwise alleged:

1. "Access device" means a code, account number, personal identification number ("PIN"), cash verification value number ("CVV"), or other means of account access, including that which may be electronically encoded onto a magnetic strip, or "mag strip," embedded on a credit, debit, or gift card, or hotel key, that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or to initiate a transfer or withdrawal of funds, all as more fully defined in Title 18, United States Code, Section 1029(e).

2. "Cashier" is an individual who acquires access devices and related personal identification information that has been obtained by fraud or other illegal means, including "phishing" or "smishing," as defined herein. A cashier uses fraudulently or illegally obtained access devices and related personal identification information to create counterfeit credit, debit, or gift cards by using encoding software and encoders to record over or re-encode the magnetic strips (or "mag" strips) on the back of legitimately issued credit, debit, or gift cards, or on hotel keys or blank plastic cards that look like ordinary access cards. Once a cashier creates these counterfeit cards, the cards can be used to obtain cash from an automated teller machine ("ATM") or cash or goods at a point of sale ("POS") terminal in a

retail establishment.

3. "Chat" is a real-time written communication over the Internet between two or more parties using software such as "ICQ" (based on the phrase, "I seek you") or AOL Instant Messenger ("AIM"). Parties to chats usually subscribe to chat services and participate in chat sessions using a "screen name" rather than by their legally given name.

4. "Counterfeit access device" means any access device that is counterfeit, fictitious, altered, or forged, all as more fully defined in Title 18, United States Code, Section 1029(e)(2).

5. "Unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained with the intent to defraud, as defined in Title 18, United States Code, Section 1029(e)(3).

6. "Device-making equipment" means a skimmer, encoder, or any equipment, mechanism, or impression designed or primarily used for making an access device or a counterfeit access device, all as more fully defined in Title 18, United States Code, Section 1029(e)(6).

7. "Encoder" is an electronic device that transfers or records access device and other information onto the magnetic strip on the back of a credit, debit, or gift card, or hotel key or blank plastic cards that look like ordinary access cards. While an encoder may be used legitimately, such as by a bank, financial institution, or hotel to create an access device for a legitimate customer, an encoder is a key tool of the counterfeit

and unauthorized access device trade and is used by criminals to manufacture counterfeit and unauthorized access devices by encoding access device cards with fraudulently obtained access device information.

8. "Encoding software" is computer software that can be purchased or downloaded for free (also known as "freeware" or "shareware") on the Internet and which is used along with an encoder to re-encode credit, debit, or gift cards, or hotel keys or blank plastic cards that look like ordinary access cards.

9. "IAD" is short for "illegally obtained access device," and means an access device, as defined hereinabove, that was obtained by fraudulent or illegal means including by spamming, phishing, or smishing as defined herein. A "cashable" IAD means an IAD that can be readily used, but usually with a short shelf-life, to obtain cash at ATMs or POS terminals.

10. "PII" as used herein means "personal identification information" and includes a name, address, date of birth, social security number, mother's maiden name, Internet login code or password, driver's license number, or other means of identification commonly provided by an individual in connection with obtaining a bank or financial account, including an account for which transactions may be effected by use of an access device.

11. "Phishing" is an attempt to fraudulently acquire access devices or PII over the Internet. Customers of financial institutions, as well as EBay, Paypal, and online banks are common targets of phishing attacks. Phishing is typically

carried out first by spamming, i.e., mass emailing, as defined herein, and often directs victims to enter details at a website that appears to be legitimately hosted by the financial institution where the victim has an account. In fact, the website is fraudulent and was solely designed to harvest access devices and PII in order to drain victims' financial accounts.

12. "Runner" is an individual who is retained by a cashier to test and use cashable IADs and to wire-transfer the proceeds obtained from using cashable IADs back to the supplier who initially obtained the IAD.

13. "Smishing" is short for phishing via Short Message Service ("SMS") text messaging. SMS text messaging is a worldwide and universally used means to send and receive text messages over the Internet or over wireless systems to cellular phones. Similar to phishing, smishing is an attempt to fraudulently acquire access devices or PII. In a smishing attack, for example, the attacker attempts to elicit a response from the victim to an SMS text message sent to the victim's cell phone, such as the following: "We're confirming that you've signed up for our service. You will be charged $2 per day unless you cancel your order on this URL (universal resource locator, an the Internet domain address): "www.trustme.com." When visiting the URL, victims are prompted to "click" an icon or link. Often times, this results in downloading a program into the victim's computer that harvests and sends to the smisher access devices and PII that will be used to create cashable IADs.

14. "Spam" is unsolicited email or text messages usually

sent in bulk and as part of a phishing or smishing attack. "Spammers" are individuals who send out spam to lure respondents to phishing or similar fraudulent sites. Spammers are able to purchase bulk quantities of email addresses, sometimes as many as one million email addresses, for as little as a few hundred dollars. Spammers oftentimes also design, post, and/or host bogus phishing sites on the Internet.

15. "Supplier" is an individual who fraudulently acquires access device information, including by means of spamming, phishing, and/or smishing. A supplier engages in Internet chat with one or more cashiers and supplies IADs to cashiers who, in turn, create cashable IADs and wire transfer to the suppliers a percentage of the illegal proceeds gained from using the cashable IADs to obtain cash from ATMs or POS terminals.

16. "WU" means "Western Union," and "MG" means "Moneygram." As used herein, WU and MG, as well as "VCOM," are money transfer services that make international wire transfers for a fee.

COUNT ONE

[18 U.S.C. § 1962(d)]

(Racketeering Conspiracy)

1. The Grand Jury realleges and incorporates herein by reference the General Allegations and Definitions of this indictment, as though fully set forth herein.

THE RACKETEERING ENTERPRISE

2. At various times relevant to this indictment, Seung Wook Lee, also known as ("aka") Brian Lee, aka "Phucked2" (hereinafter "Lee"), and defendants HIEP THANH TRAN, aka John Tran, aka Sam Lam, (hereinafter "defendant TRAN"), SORIN ALIN PANAIT, aka "scumpic4u," (hereinafter "defendant PANAIT"), STEFAN SORIN ILINCA, aka "AzZ," aka "Kahn," aka "Kahnpath" (hereinafter "defendant ILINCA"), HASSAN PARVEZ, aka "XID" (hereinafter "defendant PARVEZ"), COSTEL BULUGEA, aka "The.Vortex" (hereinafter "defendant BULUGEA"), NICOLAE DRAGOS DRAGHICI, aka Marius Bogdan Natasie, aka "Nonick" (hereinafter "defendant N. DRAGHICI"), DIDI GABRIEL CONSTANTIN, aka "StauLaSoare," aka "Estaulasoare," aka "snoop" (hereinafter "defendant CONSTANTIN"), FLORIN GEORGEL SPIRU, aka "niggaplease" (hereinafter "defendant SPIRU"), MARIAN DANIEL CIULEAN, aka "spuickeru" (hereinafter "defendant CIULEAN"), FNU LNU, aka "Cryptmaster" (hereinafter defendant "CRYPTMASTER"), FNU LNU, aka "SeleQtor" (hereinafter "defendant SELEQTOR"), IRINEL NICUSOR STANCU, aka "sicaalex" (hereinafter "defendant STANCU"), PETRU BOGDAN BELBITA, aka "CA is SK," aka "Robert Wilson" (hereinafter "defendant BELBITA"), and others known and unknown to the Grand Jury, were members and

associates of a criminal enterprise whose members and associates engaged in diverse criminal activities including, but not limited to, bank fraud, in violation of Title 18, United States Code, Section 1344; production, use, and trafficking in counterfeit access devices, in violation of Title 18, United States Code, Section 1029(a)(1); and possession of device-making equipment, in violation of Title 18 United States Code, Section 1029(a)(4), and which operated in the Central District of California, and elsewhere in the United States, and in the countries of Romania, Canada, Portugal, Pakistan, and elsewhere.

3. The above-referenced criminal organization, including its leadership, members, and associates, constituted an "enterprise," as defined by Title 18, United States Code, Section 1961(4)(hereinafter "the Enterprise"), that is, a group of individuals associated in fact. The Enterprise constituted an ongoing organization whose members functioned as a continuing unit for a common purpose of achieving the objectives of the Enterprise. This Enterprise was engaged in, and its activities affected, interstate and foreign commerce.

4. The Enterprise was bound together by, among other things, the members' and associates' common interest, knowledge, and usage of the Internet; common methods of fraudulently obtaining access devices, i.e., by spamming, phishing, and smishing; common methods of converting fraudulently obtained access devices into useable counterfeit access devices by using encoders and encoding software to re-encode access device and proprietary information onto the mag strips of credit, debit, and

gift cards, or hotel keys; common methods of obtaining cash through use of fraudulent, counterfeit, and unauthorized access devices; and a common purpose of generating criminal proceeds and obtaining goods and services through the conduct of the above-listed criminal activities. Members and associates of the Enterprise regularly used and were bound together for the exchange of fraudulently obtained access device information over the Internet, a world-wide network of computers, and members and associates regularly used the services of world-wide money transfer services, such as Western Union, in order to transfer and conceal the proceeds of their unlawful activities as alleged herein.

PURPOSES OF THE ENTERPRISE

5. The purposes of the Enterprise included at least the following:

a. Enriching and financially supporting the members and associates of the Enterprise through the fraudulent activities of spamming, phishing, and smishing; the unauthorized access and exceeding the unauthorized access of protected computers; the illegal manufacturing and use of counterfeit and unauthorized access devices from which criminal proceeds were generated and goods and services were fraudulently obtained;

b. Strengthening and expanding the relationships of the members and associates by, among other things, creating and maintaining a world-wide market for the sale of counterfeit or unauthorized access devices obtained through spamming, phishing, and smishing schemes, from which members and associates of the

Enterprise could profit;

c. Fraudulently concealing and disguising proceeds of the Enterprise's unlawful activities; and

d. Promoting and enhancing the Enterprise and its members' and associates' activities and lifestyles through the above-referenced criminal activity.

ROLES OF THE DEFENDANTS AND MEANS, METHODS, ORGANIZATIONAL STRUCTURE, OPERATION, AND MANAGEMENT OF THE ENTERPRISE

6. The defendants participated in the operation and management of the Enterprise. The defendants and other persons employed by and associated with the Enterprise functioned in the following roles, and the Enterprise was organized, structured, operated, and managed by the following means and methods:

a. Lee, operating in Glendora and Huntington Beach, in the Central District of California, and elsewhere, was a cashier for the Enterprise. Lee would communicate via Internet chat or email with other members and associates of the Enterprise located in Romania, and elsewhere, who, as suppliers, would provide Lee and others with IADs that members and associates of the Enterprise, and others, would illegally and fraudulently obtain by spamming, phishing, and smishing attacks carried out against holders of bank and credit card accounts located primarily in the United States. Lee would also assist other members and associates of the Enterprise by indicating which financial institutions might be ripe for phishing attacks. Lee, and other members and associates of the Enterprise, would, in

turn, use encoding software and encoders to re-encode the mag strips on credit, debit, and gift cards, as well as on hotel keys and blank card stock, to create cashable IADs. Lee, and others acting at his direction, including Leonard Gonzales, aka "Bonecrusher," and Rolando Soriano, aka "Loco," aka Danny Villalopez, acting as runners, would then use the cashable IADs to withdraw money from ATMs and at POS terminals and/or to purchase goods and services. Lee would then keep a percentage of the cash proceeds obtained from the use of the IADs and Lee, and others acting at his direction, would wire-transfer a percentage of illegal proceeds to the suppliers in Romania and elsewhere. Lee would also distribute a portion of the proceeds to runners as their compensation for service to the Enterprise.

b. Defendant TRAN, operating in Fullerton, in the Central District of California, and elsewhere, was, like Lee, a cashier for the Enterprise. Defendant TRAN would also communicate via Internet chat or email with other members and associates of the Enterprise located in Romania, and elsewhere, who, as suppliers, would provide defendant TRAN and others with IADs that members and associates of the Enterprise, and others, would illegally and fraudulently obtain by spamming, phishing, and smishing attacks carried out against holders of bank and credit card accounts primarily in the United States. Like Lee, defendant TRAN, and other members and associates of the Enterprise, would, in turn, use encoding software and encoders to re-encode the mag strips on credit, debit, and gift cards, as well as on hotel keys and blank card stock, to create cashable

IADs. Defendant TRAN, and others acting at his direction, including Caroline Tath, acting as runners, would then use the IADs to withdraw money from ATMs and at POS terminals, or to purchase goods and services. Like Lee, defendant TRAN would keep a percentage of the cash proceeds obtained from the illegal withdrawals and defendant TRAN, and others acting at his direction, would wire transfer a percentage of the illegal proceeds to suppliers in Romania and elsewhere.

c. Defendant PANAIT, operating from Romania, was a supplier for the Enterprise. Defendant PANAIT would obtain access devices and PII from victim account holders by spamming and phishing. Defendant PANAIT would transmit IADs via Internet chat or email from Romania to cashiers in the United States, including Lee and defendant TRAN. For example, defendant PANAIT fraudulently obtained access devices and PII from dozens of E-Trade account holders who resided in the United States by spamming and phishing and forwarded the results of his attack to Lee. Lee, in turn, used the results to create IADs and forwarded to defendant PANAIT a portion of the cash proceeds generated from withdrawing money from E-Trade accounts using those IADs. Defendant PANAIT would at times travel to the United States to meet other members and associates of the Enterprise, including Lee, to discuss and carry out Enterprise business, such as to withdraw cash from ATMs or POS terminals using IADs that Lee created using information that PANAIT had fraudulently harvested.

d. Defendant ILINCA, operating from Romania, was also a supplier for the Enterprise. Defendant ILINCA would obtain

access devices and PII that were the product of spamming, phishing, and smishing schemes, including a fraudulent scheme exacted against dozens of North Island Federal Credit Union account holders who resided in the United States. Defendant ILINCA would transmit the IADs to Lee over the Internet in exchange for a percentage of cash proceeds that Lee, and others, would obtain by creating and using cashable IADs.

e. Defendant PARVEZ, operating from Karachi, Pakistan, was also a supplier for the Enterprise who would obtain access devices and PII that were the product of spamming, phishing, and smishing schemes. Defendant PARVEZ would transmit IADs via Internet chat or email from Pakistan to Lee in the United States in exchange for a percentage of cash proceeds that Lee, and others, would obtain by creating and using cashable IADs.

f. Defendant BULUGEA, operating from Romania, was also a supplier for the Enterprise who would obtain access devices and PII that were the product of spamming, phishing, and smishing schemes. Defendant BULUGEA would transmit IADs via Internet chat or email from Romania to Lee in the United States in exchange for a percentage of cash proceeds that Lee, and others, would obtain by creating and using cashable IADs.

g. Defendant N. DRAGHICI, operating from Romania, was also a supplier for the Enterprise who would obtain access devices and PII that were the product of spamming, phishing, and smishing schemes. Defendant N. DRAGHICI would transmit IADs via Internet chat or email from Romania to Lee and defendant TRAN in

the United States in exchange for a percentage of cash proceeds that Lee and defendant TRAN, and others, would obtain by creating and using cashable IADs.

h. Defendant CONSTANTIN, operating from Romania and Portugal, was also a supplier for the Enterprise. Defendant CONSTANTIN would obtain access devices and PII that were the product of spamming, phishing, and smishing schemes. Defendant CONSTANTIN also "networked" with other suppliers in Europe to gather IADs for forwarding to Lee and other "cashiers." Like other suppliers, defendant CONSTANTIN would send IADs via Internet "chat" or email from Romania and Portugal to cashiers, including Lee, in the United States in exchange for a percentage of cash proceeds that Lee, and others, would obtain by creating and using cashable IADs.

i. Defendant SPIRU, operating from Romania, was also a supplier for the Enterprise. Defendant SPIRU would obtain access devices that were the product of spamming, phishing, and smishing schemes and would transmit IADs over the Internet that were the product of such attacks to Lee and defendant TRAN in exchange for a percentage of cash proceeds that Lee and defendant TRAN, and others, would obtain by creating and using cashable IADs.

j. Defendant CIULEAN, operating from Romania, was also a supplier for the Enterprise who would obtain IADs by spamming and phishing. Defendant CIULEAN would obtain access devices that were the product of spamming, phishing, and smishing schemes and would transmit IADs over the Internet that were the

product of such attacks to Lee in exchange for a percentage of cash proceeds that Lee, and others, would obtain by creating and using cashable IADs.

k. Defendant CRYPTMASTER, operating from Romania, was also a supplier for the Enterprise. Defendant CRYPTMASTER would obtain access devices that were the product of spamming, phishing, and smishing schemes. Defendant CRYPTMASTER would transmit IADs via Internet chat or email from Romania to Lee and defendant TRAN in the United States in exchange for a percentage of cash proceeds that Lee and defendant TRAN, and others, would obtain by creating and using cashable IADs.

l. Defendant SELEQTOR, operating from Romania, was also a supplier for the Enterprise. Defendant SELEQTOR would obtain access devices that were the product of spamming, phishing, and smishing schemes. Defendant SELEQTOR would transmit IADs via Internet chat or email from Romania to Lee in exchange for a percentage of cash proceeds which Lee, and others, would obtain by creating and using cashable IADs.

m. Defendant STANCU, operating from Romania, was also a supplier for the Enterprise. Defendant STANCU would obtain access devices that were the product of spamming, phishing, and smishing schemes. Defendant STANCU would transmit IADs via Internet chat or email from Romania to Lee and defendant TRAN in the United States in exchange for a percentage of cash proceeds that Lee and defendant TRAN, and others, would obtain by creating and using cashable IADs.

n. Defendant BELBITA, operating from Canada and

Romania, was also a supplier for the Enterprise. Defendant BELBITA would obtain access devices that were the product of spamming, phishing, and smishing schemes. Defendant BELBITA would use "collector" email accounts to amass quantities of fraudulently obtained access devices and personal financial information and would transmit those IADs via Internet chat or email to cashiers, including Lee and defendant TRAN, in exchange for a percentage of cash proceeds which Lee and defendant TRAN, and others, would obtain by creating and using cashable IADs.

o. Spammers, phishers, and smishers, unknown to the Grand Jury and not named as defendants herein, would write and send out world-wide - over the Internet, via SMS text messaging to cell phones, or via voice mail messages - to legitimate account holders of bank and credit card accounts, fraudulent messages soliciting, based on an appearance of legitimacy, access device and other sensitive information from which, when received, the Enterprise would generate its income.

THE RACKETEERING CONSPIRACY

7. Beginning at a time unknown to the Grand Jury and continuing until on or about the date of this indictment, in the Central District of California and elsewhere, defendants TRAN, PANAIT, ILINCA, PARVEZ, BULUGEA, N. DRAGHICI, CONSTANTIN, SPIRU, CIULEAN, CRYPTMASTER, SELEQTOR, STANCU, BELBITA, and others known and unknown to the Grand Jury, being persons employed by and associated with the Enterprise described above, an enterprise, which was engaged in, and the activities of which affected interstate and foreign commerce, did knowingly and willfully

conspire and agree with each other and with other persons known and unknown to the Grand Jury, to violate Title 18, United States Code, Section 1962(c), that is, to conduct and participate, directly and indirectly, in the conduct of the affairs of the Enterprise through a pattern of racketeering activity, as that term is defined in Title 18, United States Code, Sections 1961(1) and 1961(5), consisting of multiple acts indictable under the following provisions of federal law: 18 U.S.C. § 1344 (bank fraud); 18 U.S.C. § 1029(a)(1)(Production, Use and Trafficking in Counterfeit Access Devices); and 18 U.S.C. § 1029(a)(4) (Possession of Device-Making Equipment).

It was a part of the conspiracy that each defendant agreed that a conspirator would commit at least two acts of racketeering activity in the conduct of the affairs of the Enterprise.

///

///

///

///

///

///

///

///

///

///

///

///

///

OVERT ACTS

In furtherance of the racketeering conspiracy as alleged herein, and to effect the objects thereof, the defendants and their co-conspirators committed and caused to be committed the following overt acts, among others, on or about the following dates, in the Central District of California, and elsewhere:

Trafficking in IADs

Internet Chats Between Cashiers and Suppliers Regarding Spamming

1. On or about April 9, 2006, defendants TRAN and N. DRAGHICI participated in an Internet chat in which they discussed sending spam to obtain access devices.

2. On or about April 13, 2006, defendant TRAN participated in an Internet chat in which the terms of splitting the proceeds from cashable IADs were defined as "5050" and a chat participant stated, "I will start spamming for it now."

3. On or about August 2, 2006, defendants TRAN and PANAIT participated in an Internet chat in which they discussed spamming to mount a phishing attack and defendant PANAIT provided defendant TRAN with IADs, stating, among other things, "bro this are from my spam . . . super fresh . . . I will spam more . . . [I] spammed like hell . . . used 7 remote desktops and 13 smpt servers . ., 5 root . . . [and] sent over 1.3 million emails," and defendant TRAN stated, among other things, "bro, spam one of those banks please, they are cashable."

4. On or about August 2, 2006, defendants TRAN and PANAIT participated in an Internet chat in which they discussed

"hijack[ing] their homepage," referring to mounting a phishing attack against a financial institution in order to obtain IADs.

5. On or about August 2, 2006, defendants TRAN and PANAIT participated in an Internet chat in which defendant PANAIT warned that it was easier to use IADs to withdraw money from ATMs in the United States because, in Romania, "every day somebody is going to jail because of this . . . that [is] why the police is looking for atm robbers . . ."

6. On or about August 2, 2006, defendants TRAN and PANAIT participated in an Internet chat in which defendant PANAIT asked defendant TRAN, "how do u call there the thing u put on a atm mouth to copy a cc . . and a small camera to get the pin . . ," and defendant TRAN responded, "skimmer."

7. On or about May 2, 2007, Lee and defendant CONSTANTIN participated in an Internet chat in which defendant CONSTANTIN identified a new bank to "spam" and defendant CONSTANTIN described the amount of money available by spamming.

8. On or about January 9, 2008, Lee participated in an Internet chat with "cashiecashie," in which they discussed meeting in a Pomona hotel to spam with Rolando Soriano.

9. On or about February 2, 2008, Lee and defendant N. DRAGHICI participated in an Internet chat in which they exchanged their telephone numbers and defendant N. DRAGHICI asked Lee to "give me a good bank to spam."

Supplier PANAIT

10. On or about August 2, 2006, defendants TRAN and PANAIT participated in an Internet chat in which they discussed, among

other things, spamming, IADs, and converting IADs into cash.

11. In or about May 2007, defendant PANAIT traveled from Romania to Orange County, California, to use IADs with Lee.

12. In or about August 2007, defendant PANAIT traveled from Romania to Orange County, California, to use IADs with Lee.

13. In or about August 2007, defendant PANAIT purchased a Boost Mobile phone, with the assigned telephone number (714) 391-7616, for Lee for use in communicating regarding IADs.

14. On or about January 7, 2008, defendant PANAIT sent Lee over the Internet a file entitled, "new from scump" which contained eight IADs, including debit card number xxxx-xxxx-xxxx-2470, issued by Jeffco Schools Credit Union, and related PII.

15. On or about January 9, 2008, Lee and defendant PANAIT participated in an Internet chat in which they discussed using an "mtcn" (a "money transfer control number" related to WU wire transfers) related to IADs and defendant PANAIT solicited Lee to engage in further business opportunities, including to invest in counterfeit cigarette trafficking in Western Europe.

16. On or about January 9, 2008, defendant PANAIT sent Lee over the Internet a file entitled, "2 points" which contained a IADs including access card number xxxx-xxxx-xxxx-0731, issued by Pointbank, and related PII, and access card number xxxx-xxxx-xxxx-0731, issued by Bowdoinham Federal Credit Union, and related PII.

17. On or about January 13, 2008, defendant PANAIT sent Lee over the Internet a file entitled, "arizones 8" which

///

contained IADs including access card number xxxx-xxxx-xxxx-4972, issued by Arizona Federal Credit union, and related PII.

18. On or about January 26, 2008, Lee and defendant PANAIT participated in an Internet chat in which defendant PANAIT offered to hack a police database to expunge Lee's police record.

19. On or about February 15, 2008, defendant PANAIT sent Lee over the Internet a file entitled, "cap 1.txt" which contained approximately 260 IADs including access card number xxxx-xxxx-xxxx-7694, issued by Capital One Bank.

Supplier ILINCA

20. On or about April 30, 2007, Lee and defendant ILINCA participated in an Internet chat in which Lee asked defendant ILINCA if defendant ILINCA had received money sent by Lee as proceeds from the use of IADs supplied by defendant ILINCA.

21. On or about September 5, 2007, defendant ILINCA in Romania, called the Boost Mobile telephone number (714) 391-7616, which defendant PANAIT had purchased for Lee.

22. On or about October 1, 2007, defendant ILINCA in Romania called telephone number (714) 492-6884, which defendant TRAN had stated was his telephone number.

23. On or about January 10, 2008, Lee and defendant ILINCA participated in an Internet chat in which defendant ILINCA asked Lee to buy two servers for "email harvesting" for the purpose of fraudulently obtaining access devices.

24. On or about January 17, 2008, defendant ILINCA sent Lee over the Internet a file entitled, "new testers from azz" which contained approximately 60 IADs, each with related PII.

25. On or about January 28, 2008, Lee participated in an Internet chat with "IntrUd3r" in which "IntrUd3r" stated that he was a friend of defendants ILINCA and CONSTANTIN.

26. On or about March 11, 2008, defendant ILINCA sent to Lee over the Internet a file entitled, "15 new north islands.txt" which contained approximately 15 IADs issued by North Island Credit Union including access device number xxxx-xxxx-xxxx-5971 and its associated PIN.

Supplier PARVEZ

27. On or about April 13, 2006, defendant PARVEZ sent to defendant TRAN over the Internet a file entitled, "new langley fcu" which contained two IADs including access device number xxxx-xxxx-xxxx-2129, issued by Langley Federal Credit Union.

28. On or about January 10, 2008, defendant PARVEZ sent to Lee over the Internet a file entitled, "xid mixed point" which contained seven IADs including access device number xxxx-xxxx-xxxx-9217, issued by Capital One Bank.

29. On or about January 10, 2008, defendant PARVEZ sent to Lee over the Internet a file entitled, "xid point new" which contained one IAD, namely, access device number xxxx-xxxx-xxxx-9158, issued by Pointbank, and related PII.

30. On or about January 14, 2008, defendant PARVEZ sent to LEE over the Internet a file entitled, "new langley fcu" which contained two IADs, including access device number xxxx-xxxx-xxxx-2129, issued by Langley Federal Credit Union.

31. On or about January 16, 2008, defendant PARVEZ sent to Lee over the Internet a file entitled, "xid paki" which contained

approximately 40 fraudulently obtained access device numbers, including number xxxx-xxxx-xxxx-4748, issued by Citibank, as well as related email addresses and PINs.

32. On or about February 10, 2008, Lee created the file, "xid bins," based on IADs provided to him by defendant PARVEZ, identifying approximately 25 access device card issuers and the ATM and POS terminal withdrawal limits imposed by each such issuer.

33. On or about February 11, 2008, Lee, defendant PARVEZ, and defendant N. DRAGHICI participated in an Internet chat in which they discussed IADs including access device numbers xxxx-xxxx-xxxx-6897 and xxxx-xxxx-xxxx-0490, issued by Pointbank, and Lee's computer file entitled, "new text document" which contained IADs.

34. On or about February 15, 2008, Lee and defendant PARVEZ participated in an Internet chat in which they discussed approximately 170 fraudulently obtained access devices identified in Lee's computer file entitled, "xid files," including access device number xxxx-xxxx-xxxx-3253, issued by the Franklin Mint Federal Credit Union, and related PII.

35. On or about February 24, 2008, Lee and defendant PARVEZ participated in an Internet chat in which they discussed IADs including access device number xxxx-xxxx-xxxx-0706, issued by Valley National Bank.

36. On or about March 1, 2008, Lee and defendant PARVEZ participated in an Internet chat in which they discussed fraudulently obtained access devices issued by the Franklin Mint.

Supplier BULUGEA

37. On or about May 1, 2007, Lee and defendant BULUGEA participated in an Internet chat in which defendant BULUGEA asked Lee if he (Lee) had "any luck" using PINs for federal credit union access devices.

38. On or about May 3, 2007, Lee and defendant BULUGEA participated in an Internet chat in which defendant BULUGEA asked Lee if he (Lee) had yet withdrawn any money from ATMs or POS terminals using IADs supplied by defendant BULUGEA.

39. On or about May 3, 2007, Lee and defendant BULUGEA participated in an Internet chat in which defendant BULUGEA sent Lee five IADs including access device number xxxx-xxxx-xxxx-6715, issued by American National Bank of Texas, and related PII.

40. On or about January 7, 2008, defendant BULUGEA sent to Lee over the Internet a file entitled, "vortex 3 mountains" which contained three IADs, including access device number xxxx-xxxx-xxxx-6382, issued by Mountain America Credit Union.

41. On or about January 8, 2008, defendant BULUGEA sent to Lee over the Internet a file entitled, "mountain 6 new" which contained seven fraudulently obtained access device numbers and related PII, including number xxxx-xxxx-xxxx-2380, issued by Mountain America Credit Union.

42. On or about January 9, 2008, Lee and defendant BULUGEA participated in an Internet chat in which defendant BULUGEA asked Lee if he (Lee) had "the mtcn," referring to a unique WU "money transfer control number," and further asked Lee to ask defendant TRAN to respond to defendant BULUGEA's Internet chat question.

43. On or about January 10, 2008, Lee and defendant BULUGEA participated in an Internet chat in which Lee stated that two separate "mtcn's," $2,500 each, had been sent, one by Rolando Soriano, and the other by Loi Tan Dang.

44. On or about February 1, 2008, Lee and defendant BULUGEA participated in an Internet chat in which defendant BULUGEA stated that he knew "sica," referring to defendant STANCU, "spuikeruju," referring to defendant CIULEAN, and "caronline," referring to Caroline Tath.

Supplier N. DRAGHICI

45. On or about April 9, 2006, defendants TRAN and N. DRAGHICI participated in an Internet chat in which defendant N. DRAGHICI sent to defendant TRAN the social security number for, and an access device, PIN, and CVV for, an access device duly issued by Banker's Bank to E.L., and further solicited help with spamming from defendant TRAN by stating, "help me with smtp to spam bb&t," referring to Banker's Bank & Trust.

46. On or about February 1, 2008, Lee and defendant N. DRAGHICI participated in an Internet chat in which they discussed IADs including access device xxxx-xxxx-xxxx-1468, issued by Pointbank.

47. On or about February 4, 2008, Lee and defendant N. DRAGHICI participated in an Internet chat in which defendant N. DRAGHICI sent Lee IADs including access device xxxx-xxxx-xxxx-2746, issued by or for the benefit of Payment Systems for Credit Unions, Inc.

48. On or about February 4, 2008, Lee and defendant N.

DRAGHICI participated in an Internet chat in which defendant N. DRAGHICI gave Lee the name of "Marius Bogdan Natasie" to use in communicating with defendant N. DRAGHICI.

Supplier CONSTANTIN

49. On or about May 1, 2007, defendant CONSTANTIN sent Lee over the Internet a file containing mtcn's related to the transfer of proceeds generated from the use of IADs supplied by defendant CONSTANTIN.

50. On or about May 2, 2007, defendant CONSTANTIN sent to Lee over the Internet seven IADs including access device number xxxx-xxxx-xxxx-7394 issued by Flagstar Bank.

51. On or about May 3, 2007, defendant CONSTANTIN and Lee participated in an Internet chat in which Lee stated that defendant CONSTANTIN had provided the wrong PIN for an IAD that defendant CONSTANTIN had provided.

52. On or about November 25, 2007, defendant CONSTANTIN and Lee participated in an Internet chat in which defendant CONSTANTIN sent Lee seven IADs including access number xxxx-xxxx-xxxx-8431, issued by Premier Credit Union.

53. On or about January 10, 2008, Lee and defendant CONSTANTIN participated in an Internet chat in that Lee stated that three separate "MTCN's" had been sent as payment for the supply of IADs by defendant CONSTANTIN, one by Lee for $980, one by Rolando Soriano, for $2,320, and one by Loi Tan Dang, for $1,500.

54. On or about January 28, 2008, Lee and defendant CONSTANTIN participated in an Internet chat in which defendant

CONSTANTIN stated that "IntrUd3r" was a Romanian spammer.

Supplier CIULEAN

55. On or about January 13, 2008, defendant CIULEAN sent Lee over the Internet a file entitled, "payment systems" that contained two fraudulently obtained access device numbers including number xxxx-xxxx-xxxx-0385, issued by or for the benefit of Payment Systems for Credit Union, and related PII.

56. Between on or about January 25, 2008 and through on or about March 10, 2008, defendant CIULEAN sent to Lee over the Internet approximately 31 files containing IADs.

57. On or about January 30, 2008, Lee and defendant CIULEAN participated in an Internet chat in which defendant CIULEAN asked Lee for the status of payment due defendant CIULEAN for IADs that defendant CIULEAN had sent to Lee and defendant CIULEAN gave Lee his (CIULEAN's) telephone number in Romania.

58. On or about February 17, 2008, defendant CIULEAN sent Lee over the Internet an IAD, namely, access device number xxxx-xxxx-xxxx-4386, issued by Langley Federal Credit Union.

59. On or about March 10, 2008, defendant CIULEAN sent Lee over the Internet an IAD, namely, access device number xxxx-xxxx-xxxx-6938, issued by Allegheny Federal Credit Union.

Supplier SPIRU

60. On or about April 17, 2007, defendant SPIRU sent Lee over the Internet approximately seven IADs including access device number xxxx-xxxx-xxxx-2105, issued by Southwest Corporate Federal Credit Union, and related PII.

61. On or about June 3, 2007, defendant SPIRU sent Lee

over the Internet the result of a phishing attack that contained approximately thirteen IADs including access device number xxxx-xxxx-xxxx-7749, issued by Telco Credit Union & Affiliates, and related PII.

62. On or about November 4, 2007, defendant SPIRU sent Lee over the Internet approximately thirteen IADs including access device number xxxx-xxxx-xxxx-9794, issued by First Merit Bank, and related PII.

Supplier CRYPTMASTER

63. On or about February 26, 2007, Lee and defendant CRYPTMASTER participated in an Internet chat in which defendant CRYPTMASTER sent Lee approximately five IADs, including access device number xxxx-xxxx-xxxx-0709, issued by Teacher's Credit Union.

64. On or about April 30, 2007, Lee and defendant CRYPTMASTER participated in an Internet chat in which they discussed algorithms necessary to use IADs.

65. On or about April 30, 2007, Lee and defendant CRYPTMASTER participated in an Internet chat in which defendant CRYPTMASTER sent Lee two IADs obtained from a phishing attack against holders of accounts at Downey Savings & Loan, including access device number xxxx-xxxx-xxxx-6876.

66. In or about May 2007, Lee and defendant CRYPTMASTER participated in an Internet chat in which defendant CRYPTMASTER sent Lee approximately 100 IADs that were the product of a phishing attack against holders of accounts at Capital One Bank, including access device number xxxx-xxxx-xxxx-7128.

67. On or about May 2, 2007, Lee and defendant CRYPTMASTER participated in an Internet chat in which they discussed using "Epass" to transfer proceeds from the use of IADs supplied by defendant CRYPTMASTER.

68. On or about May 2, 2007, Lee and defendant CRYPTMASTER participated in an Internet chat in which LEE gave defendant CRYPTMASTER the Western Union MTCN relating to a transfer of a portion of the proceeds from the use of IADs supplied by CRYPTMASTER.

69. On or about May 3, 2007, Lee and defendant CRYPTMASTER participated in an Internet chat in which they discussed using "epassporte" to transfer proceeds from the use of IADs and Lee gave defendant CRYPTMASTER login information to "epassporte."

Supplier SELEQTOR

70. On or about May 1, 2007, Lee and defendant SELEQTOR participated in an Internet chat in which they discussed obtaining money from ATMs using IADs and phishing against Downey Savings & Loan.

71. On or about April 2007, defendant SELEQTOR sent Lee an IAD with its associated PIN and CVV, which had been obtained from a phishing attack against Capital One Bank.

72. On or about April 17, 2007, Lee and defendant SELEQTOR participated in an Internet chat in which defendant SELEQTOR sent Lee PayPal logins and associated information from third parties.

73. On or about May 3, 2007, Lee and defendant SELEQTOR participated in an Internet chat in which defendant SELEQTOR sent Lee approximately 19 IADs with related PII, including IADs from

First U.S.A. Bank, Capital One Bank, and Bank of America.

74. On or about July 9, 2007, Lee and defendant SELEQTOR participated in an Internet chat in which defendant SELEQTOR sent Lee an IAD with related PII, which had been obtained from a phishing attack against customers of E-Trade.

75. On or about January 10, 2008, Lee and defendant SELEQTOR participated in an Internet chat in which they discussed fraudulently using access devices issued by Downey Savings & Loan Association.

76. On or about January 12, 2008, defendant SELEQTOR sent Lee over the Internet two IADs that were obtained by a phishing attack against holders of accounts at Downey Savings & Loan, including access device number xxxx-xxxx-xxxx-4448, and related PII.

Supplier STANCU

77. On or about December 8, 2005, defendants TRAN and STANCU participated in an Internet chat in which defendant STANCU sent defendant TRAN four IADs and related PII and stated, "send me the money . . . and tomorrow . . . You have another 10," referring to another ten IADs.

78. On or about April 13, 2006, defendants TRAN and STANCU participated in an Internet chat in which they discussed transferring money using Western Union.

79. On or about August 22, 2007, Lee and defendant STANCU participated in an Internet chat in which defendant STANCU sent Lee approximately sixteen IADs, including access device number xxxx-xxxx-xxxx-0779, issued by Boeing Employees' Credit Union,

and related PII.

80. On or about December 17, 2007, Lee and defendant STANCU participated in an Internet chat in defendant STANCU sent Lee approximately eight IADs, including access device number xxxx-xxxx-xxxx-8794, issued by Nasa Federal Credit Union, and related PII.

Supplier BELBITA

81. In or about February 2006, defendant BELBITA received over the Internet an email that contained tools designed for phishing against Bank of America customers.

82. In or about March, August, and October 2006, defendant BELBITA had access through third parties, including Ovidiu-Ionut Nicola-Roman, to shared email collector accounts including "raize2hell@yahoo.com," and "fly4hell@yahoo.com," each of which contained over approximately 228 email messages that contained credit card numbers, expiration dates, CVV's, PIN's, names, addresses, telephone numbers, dates of birth, and Social Security numbers of individuals who had responded to phishing attacks.

83. On or about December 20, 2006, defendant BELBITA asked defendant TRAN to create a fraudulent driver's license to enable defendant BELBITA to freely travel between Romania and Canada.

84. In or about December 2006, defendant TRAN created a fraudulent California driver's license for defendant BELBITA, bearing number B4155321, in the name of Robert Wilson.

85. In or about December 2006, Lee, at the direction of defendant TRAN, mailed a fraudulent California driver's license

///

in the name of Robert Wilson to defendant BELBITA, in Canada.

86. On or about March 21 and 22, 2007, defendant BELBITA participated in a phishing attack that generated approximately 206 responses from holders of bank and credit card accounts who provided access device and sensitive personal information, including S.W., who provided access device number xxxx-xxxx-xxxx-5463, from which defendant BELBITA and other members of the Enterprise intended to create cashable IADs.

Possession of Device-Making Equipment

87. On or about August 2, 2006, defendant TRAN and Caroline Tath possessed device-making equipment, including a Dell Inspiron laptop computer, serial number 9CPHF91; a Hewlett-Packard laptop computer, serial number CND5470C4V; a Logitech flash drive; a Gigatech flash drive; a Lexar flash drive; an MSR 206 encoder; an Operah card reader; a Western Digital hard drive; and numerous access device cards.

88. On or about August 2, 2006, defendant TRAN possessed software entitled, "CC2Bank 1.3.," to check the bank identification number for access devices to create IADs.

89. On or about August 2, 2006, defendant TRAN possessed software entitled, "MSR206 Utility," which he intended to use for re-encoding access devices.

90. On or about August 2, 2006, defendant TRAN possessed approximately 50 counterfeit driver licenses on computer files, identified as file numbers 0208-0264.jpg, on defendant TRAN's Sony Vaio laptop computer; an alphabetical listing of over 1,000 financial institutions with their respective bank identification

numbers, identified as file number 0180.db on defendant TRAN's Sony Vaio laptop computer; and an alphabetical listing of over 1,000 financial institutions with their respective bank identification numbers ("BIN"), identified as file number 0188.db on defendant TRAN's Sony Vaio laptop computer.

91. In or about January 2007, defendant TRAN traveled with Lee to Downey, California, to purchase an MSR encoder to be used to make cashable IADs.

92. In or about January 2007, defendant TRAN gave Lee a software program entitled, "TheJermMSR206" to operate an MSR encoder in order to make IADs.

93. On or about March 10, 2008, Lee possessed device-making equipment, including approximately 51 access cards; a Sony Vaio Silver/Orange laptop computer; encoding software; an MSR505C encoder; and access cards for re-encoding into IADs.

94. On or about March 10, 2008, Lee obtained over the Internet approximately 1,000,000 email addresses for the price of $400 for the purpose of mounting a phishing attack.

95. On or about March 11, 2008, Lee possessed device-making equipment, including a Sony Vaio Silver/Blue laptop computer, serial number C101A9TA; a Sony Vaio Silver/Red laptop computer, serial number C101NWG8; an MSR505C encoder; and access cards for re-encoding.

Possession and Use of IADs

96. On or about March 14, 2006, defendant TRAN and Caroline Tath possessed a counterfeit access device, namely, Visa debit access card number xxxx-xxxx-xxxx-3285, issued to N.L.

97. On or about March 14, 2006, defendant TRAN and Caroline Tath possessed a counterfeit access device, namely, Visa debit access card number xxxx-xxxx-xxxx-7311, issued to J.G.

98. On or about March 14, 2006, defendant TRAN and Caroline Tath possessed a counterfeit access device, namely, Visa debit access card number xxxx-xxxx-xxxx-1960, issued to F.C.

99. On or about March 14, 2006, defendant TRAN and Caroline Tath possessed a counterfeit access device, namely, Visa debit access card number xxxx-xxxx-xxxx-3758, issued to R.R.

100. On or about March 14, 2006, defendant TRAN and Caroline Tath possessed a counterfeit access device, namely, Visa debit access card number xxxx-xxxx-xxxx-7868, issued to D.J.

101. On or about July 27, 2006, defendant TRAN and Caroline Tath possessed a counterfeit access device, namely, Visa debit access card number xxxx-xxxx-xxxx-0982.

102. On or about July 27, 2006, defendant TRAN and Caroline Tath possessed a counterfeit access device, namely, Visa debit access card number xxxx-xxxx-xxxx-0725.

103. On or about July 27, 2006, defendant TRAN and Caroline Tath possessed a counterfeit access device, namely, Visa debit access card number xxxx-xxxx-xxxx-6514.

104. On or about July 27, 2006, defendant TRAN and Caroline Tath possessed a counterfeit access device, namely, Visa debit access card number xxxx-xxxx-xxxx-7240.

105. On or about September 16, 2007, Lee and Leonard Gonzales used a counterfeit access device, number xxxx-xxxx-xxxx-0382 issued by PSCU Financial Services, Inc., to purchase goods

at Walmart in Glendora, California.

106. On or about September 16, 2007, Lee and Leonard Gonzales used a counterfeit access device, number xxxx-xxxx-xxxx-7359, issued by North Island Credit Union, to purchase goods at Walmart in Glendora, California.

107. On or about March 10, 2008, Lee possessed approximately 30 counterfeit and unauthorized access devices, including All Access Visa Debit card number xxxx-xxxx-xxxx-2094.

E-Trade Phishing Attack

108. Between in or about July 2007 and September 2007, an unknown co-conspirator or co-conspirators caused spam to be sent to holders of E-Trade accounts in order to fraudulently harvest access devices and PII.

Account Holder E.C.

109. On or about July 3, 2007, an unknown co-conspirator or co-conspirators using Internet Protocol ("IP") address 76.98.87.153 made an inquiry over the Internet of the E-Trade account of E.C.

110. On or about July 5, 2007, Lee and defendant PANAIT possessed E-Trade access device number xxxx-xxxx-xxxx-7048 issued to E.C.

111. On or about July 5, 2007, Lee directed the withdrawal of cash from ATMs and POS terminals in Orange County, California, against the E-Trade account of E.C., using an IAD.

Account Holder D.D.

112. On or about July 3, 2007, an unknown co-conspirator or co-conspirators using IP address 70.251.226.209 made an

inquiry over the Internet of the E-Trade account of D.D.

113. On or about July 13, 2007, Lee and defendant PANAIT possessed E-Trade access device number xxxx-xxxx-xxxx-1761 issued to D.D.

114. On or about July 13, 2007, Lee directed the withdrawal of cash from ATMs and POS terminals in Orange County, California, against the E-Trade account of D.D., using an IAD.

Account Holder K.D.

115. On or about July 31, 2007, an unknown co-conspirator or co-conspirators using IP address 69.121.90.34 made an inquiry over the Internet of the E-Trade account of K.D.

116. On or about August 1, 2007, Lee and defendant PANAIT possessed E-Trade access device number xxxx-xxxx-xxxx-3306 issued to K.D.

117. Between on or about August 1, 2007, and August 6, 2007, Lee directed the withdrawal of cash from ATMs and POS terminals in Los Angeles and Orange Counties, California, against the E-Trade account of K.D.

Account Holder R.C.

118. On or about August 1, 2007, an unknown co-conspirator or co-conspirators using IP address 172.165.157.61 made an inquiry over the Internet of the E-Trade account of R.C.

119. On or about July 30, 2007, Lee and defendant PANAIT possessed E-Trade access device number xxxx-xxxx-xxxx-4302 issued to R.C.

120. Between on or about July 30, 2007, and August 6, 2007, Lee directed Rolando Soriano and Leonard Gonzales to

withdraw cash from ATMs and POS terminals in Las Vegas, Nevada, and Orange County, California, against the E-Trade account of R.C.

Account Holder S.P.

121. On or about August 12, 2007, an unknown co-conspirator or co-conspirators using IP addresses 59.23.225.51 and 59.6.81.173 made inquiries over the Internet of the E-Trade account of S.P.

122. On or about August 13, 2007, Lee and defendant PANAIT possessed E-Trade access device number xxxx-xxxx-xxxx-3660 issued to S.P.

123. On or about August 13, 2007, Leonard Gonzales, at the direction of Lee, conducted a balance inquiry of the E-Trade account of S.P.

124. On or about August 13, 2007, Leonard Gonzales, at the direction of Lee withdrew approximately $3,417 in cash from a POS terminal at 1100 North La Cienaga Blvd., West Hollywood, California, using an IAD made by Lee against the E-Trade account of S.P.

Account Holder B.C.

125. On or about September 2, 2007, an unknown co-conspirator or co-conspirators using IP address 200.49.174.86 attempted to make an inquiry over the Internet of the E-Trade account of B.C.

126. On or about August 31, 2007, Lee and defendant PANAIT possessed E-Trade access device number xxxx-xxxx-xxxx-3909 issued to B.C.

127. Between on or about August 31, 2007, and September 2, 2007, Lee directed the withdrawal of cash from ATMs and POS terminals in Los Angeles and Orange Counties, California, against the E-Trade account of B.C.

Phishing Attack on Credit Union One, Anchorage, Alaska

128. On or about January 14, 2008, an unknown co-conspirator or co-conspirators mounted a phishing attack against account holders at Credit Union One in Anchorage, Alaska.

129. On or about January 14, 2008, defendant ILINCA sent an email message to Lee containing the email address, personal identification number, expiration date, card verification value number, and access device number xxxx-xxxx-xxxx-9020 issued to T.H. by Credit Union One of Anchorage, Alaska.

North Island Credit Union Phishing and Smishing Attack

130. Between in or about May 2007 and on or about March 31, 2008, an unknown co-conspirator or co-conspirators mounted a phishing attack and created over 300 fraudulent websites in order to harvest access devices from holders of accounts at North Island Credit Union.

131. In or about February 2008, an unknown co-conspirator engaged in a smishing attack by sending a purported message from Verizon Wireless to be sent to D.K., the holder of an account at North Island Credit Union.

132. In or about March 2008, an unknown co-conspirator engaged in a smishing attack by sending a purported message from Verizon Wireless to be sent to V.F., the holder of an account at North Island Credit Union.

133. In or about March 2008, an unknown co-conspirator engaged in a smishing attack by sending a purported message from Verizon Wireless to be sent to J.B., the holder of an account at North Island Credit Union.

134. On or about March 10, 2008, Lee created and gave to Rolando Soriano a cashable IAD created from an access device issued by North Island Credit Union to account holder D.K.

135. On or about March 10, 2008, Lee created and gave to Rolando Soriano a cashable IAD created from an access device issued by North Island Credit Union to account holder V.F.

136. On or about March 11, 2008, Lee and defendant ILINCA possessed approximately fifteen IADs created from access devices that had been issued by North Island Credit Union to its account holders.

Langley Federal Credit Union Phishing Attack

137. In or about January 2008, Langley Federal Credit Union account holder C.S., and other Langley Federal Credit Union account holders, were victims of a phishing attack in which such account holders received spam email that directed each of them to enter access device information and PII at a phishing web site, "www.langleyfcu.org."

138. In or about January 2008, Langley Federal Credit Union account holder C.S. entered access device and PII on the phishing web site, "www.langleyfcu.org," including access device number xxxx-xxxx-xxxx-0732.

139. On or about January 18, 2008, postal money order number 12124417050 was purchased in the name of "Hiep Tran" from

the U.S. Post Office in La Habra, California, in the amount of $675.15, using Langley Federal Credit Union debit card number xxxx-xxxx-xxxx-0732, issued to C.S.

140. On or about February 28, 2008, defendant TRAN conducted balance inquiries at an Orange County Teacher's Credit Union ATM in La Habra, California, for Langley Federal Credit Union debit card account numbers xxxx-xxxx-xxxx-7952, issued to R.R.; xxxx-xxxx-xxxx-2151, issued to S.P.; and xxxx-xxxx-xxxx-1959, issued to E.W. and J.C.

141. On or about February 28, 2008, defendant TRAN withdrew the amount of $71.50 at an Orange County Teacher's Credit Union ATM in La Habra, California, using debit access device number xxxx-xxxx-xxxx-7952, issued by Langley Federal Credit Union to R.R.

142. On or about February 28, 2008, defendant TRAN purchased electronic equipment for $64.39, and a prepaid access card for $1,004.64, from a Walmart store located in La Habra, California, using debit access device number xxxx-xxxx-xxxx-1959, issued by Langley Federal Credit Union to E.W. and J.C.

Wire Transfers of Cashable IAD Proceeds to Suppliers

To Defendant PANAIT

143. On or about July 20, 2006, defendant TRAN, using the name "Sam Lam," caused to be wire transferred via MG the amount of $895 to defendant PANAIT in Romania as proceeds from the use of IADs supplied by defendant PANAIT.

144. On or about March 10, 2008, Lee caused $300.99 to be transferred from Orange County, California, to a third party at

the direction and for the benefit of defendant PANAIT.

To Defendant ILINCA

145. On or about December 4, 2005, defendant TRAN caused to be wire-transferred via VCOM the amount of $457 to defendant ILINCA in Romania, as proceeds for the use of IADs supplied by defendant ILINCA.

146. On or about March 7, 2008, Rolando Soriano at the direction of Lee caused to be wire-transferred via Western Union the amount of $2,200 to defendant ILINCA in Romania, as proceeds for the use of IADs supplied by defendant ILINCA.

To Defendant SPIRU

147. On or about October 30, 2005, defendant TRAN, using the name "John Tran," caused to be wire-transferred via Western Union the amount of $356 to defendant SPIRU in Romania as proceeds from the use of IADs supplied by defendant SPIRU.

148. On or about November 7, 2005, defendant TRAN, using the name "John Tran," caused to be wire-transferred via WU the amount of $386 to defendant SPIRU in Romania as proceeds from the use of IADs supplied by defendant SPIRU.

149. On or about November 29, 2005, defendant TRAN caused $100 to be wire-transferred from Orange County, California, to defendant SPIRU in Romania as proceeds from the use of IADs supplied by defendant SPIRU.

150. On or about December 4, 2005, defendant TRAN caused $366 to be wire-transferred from Orange County, California, to defendant SPIRU in Romania as proceeds from the use of IADs supplied by defendant SPIRU.

151. On or about December 8, 2005, defendant TRAN, using the name "John Tran," caused to be wire-transferred via WU the amount of $932 to defendant SPIRU in Romania as proceeds from the use of IADs supplied by defendant SPIRU.

152. On or about December 28, 2005, defendant TRAN caused to be wire-transferred via VCOM the amount of $932 to defendant SPIRU in Romania as proceeds from the use of IADs supplied by defendant SPIRU.

153. On or about January 13, 2006, defendant TRAN caused to be wire-transferred via VCOM the amount of $250 to defendant SPIRU as proceeds from the use of IADs supplied by defendant SPIRU.

154. On or about January 16, 2006, defendant TRAN caused to be wire-transferred via VCOM the amount of $200 to defendant SPIRU as proceeds from the use of IADs supplied by defendant SPIRU.

155. On or about February 3, 2006, defendant TRAN caused to be wire-transferred via VCOM the amount of $490 to defendant SPIRU as proceeds from the use of IADs supplied by defendant SPIRU.

156. On or about July 22, 2006, defendant TRAN, using the name "Sam Lam," caused to be wire-transferred via MG the amount of $480 to defendant SPIRU in Romania as proceeds from the use of IADs supplied by defendant SPIRU.

To Defendant STANCU

157. On or about December 8, 2005, defendant TRAN caused to be wire-transferred via VCOM the amount of $100 to defendant

STANCU as proceeds from the use of IADs supplied by defendant STANCU.

158. On or about December 22, 2005, defendant TRAN caused to be wire-transferred via VCOM the amount of $200 to defendant STANCU as proceeds from the use of IADs supplied by defendant STANCU.

159. On or about December 28, 2005, defendant TRAN caused to be wire-transferred via VCOM the amount of $100 to defendant STANCU as proceeds from the use of IADs supplied by defendant STANCU.

To Lucian Zamfirache, aka "Krobelus"

160. On or about February 16, 2006, defendant TRAN caused to be wire-transferred via VCOM the amount of $250 to Lucian Zamfirache, aka "Krobelus," as proceeds from the use of IADs supplied by Zamfirache.

161. On or about February 18, 2006, defendant TRAN caused to be wire-transferred via VCOM the amount of $400 to Lucian Zamfirache, aka "Krobelus," as proceeds from the use of IADs supplied by Zamfirache.

162. On or about February 19, 2006, defendant TRAN caused to be wire-transferred via VCOM the amount of $200 to Lucian Zamfirache, aka "Krobelus," as proceeds from the use of IADs supplied by Zamfirache.

To Defendant BULUGEA

163. On or about January 10, 2008, Lee and Rolando Soriano caused to be wire-transferred via WU the amount of $2,500 to defendant BULUGEA as proceeds for the use of IADs supplied by

defendant BULUGEA.

164. On or about January 10, 2008, Lee and Loi Tan Dang caused to be wire-transferred via WU the amount of $2,500 to defendant BULUGEA as proceeds for the use of IADs supplied by defendant BULUGEA.

Other Wire Transfers on Behalf of Suppliers

165. On or about July 12, 2006, defendant TRAN, using the name "Sam Lam," caused to be wire-transferred via MG the amount of $800 to P.D.I. in Romania as proceeds for the use of a supply of IADs.

166. On or about July 12, 2006, defendant TRAN, using the name "Sam Lam," caused to be wire-transferred via MG the amount of $800 to P.D.I. in Romania as proceeds for the use of a supply of IADs.

167. On or about July 20, 2006, defendant TRAN, using the name "Sam Lam," caused to be wire-transferred via MG the amount of $800 to D.I.C. in Romania as proceeds for the use of a supply of IADs.

168. On or about July 20, 2006, defendant TRAN, using the name "Sam Lam," caused to be wire-transferred via MG the amount of $895 to P.I.D. in Romania as proceeds for the use of a supply of IADs.

169. In or about July 2006, defendant TRAN caused to be wire-transferred via MG the amount of $1,500 to P.I.D. in Romania as proceeds for the use of a supply of IADs.

170. In or about July 2006, defendant TRAN caused to be wire-transferred via MG the amount of $2,500 to P.I.D. in Romania

as proceeds for the use of a supply of IADs.

171. On or about September 6, 2007, Leonard Gonzales, at the direction of Lee, caused to be wire-transferred via WU the amount of $300 to C.C. in Romania as proceeds from the use of IADs.

172. On or about September 6, 2007, Leonard Gonzales, at the direction of Lee, caused to be wire-transferred via WU the amount of $450 to D.I. in Romania as proceeds from the use of IADs.

173. On or about February 28, 2008, Lee, using the name "Gabriel Ion," caused $500 to be wire-transferred via WU from Las Vegas, Nevada, to R.P.A. in Romania as payment for spamming.

174. On or about February 28, 2008, Nga Ngo, aka Christine Ngo, at the direction of Lee, caused $1,200 to be wire-transferred via WU from Las Vegas, Nevada, to E.A.M. in Romania as payment for the supply of IADs.

All in violation of Title 18, United States Code, Section 1962(d).

COUNT TWO

[18 U.S.C. §1029(b)(2)]

(Conspiracy to Commit Access Device Fraud)

1. The Grand Jury re-alleges and incorporates by reference the General Allegations and Definitions; paragraphs one through six, inclusive of Count One; and Overt Acts one through 174, inclusive, of Count One, as though fully set forth herein.

OBJECTS OF THE CONSPIRACY

2. Beginning on a date unknown to the Grand Jury, and continuing to on or about the date of this indictment, in Los Angeles County and Orange County, within the Central District of California, and elsewhere, Lee and defendants TRAN, PANAIT, ILINCA, PARVEZ, BULUGEA, N. DRAGHICI, CONSTANTIN, SPIRU, CIULEAN, CRYPTMASTER, SELEQTOR, STANCU, BELBITA, ROLANDO SORIANO, aka "Loco," aka Danny Villalopez (hereinafter "SORIANO"), LEONARD GONZALES, aka "Bonecrusher" (hereinafter "GONZALES"), NGA NGO, aka Christina Ngo (hereinafter "NGO"), CAROLINE TATH (hereinafter "TATH"), SONNY DUC VO (hereinafter "VO"), LOI TAN DANG, aka Mike Dang (hereinafter "DANG"), DUNG PHAN (hereinafter "PHAN"), THAI HOANG NGUYEN (hereinafter "NGUYEN"), ALEX CHUNG LUONG (hereinafter "LUONG"), FNU LNU, aka "PaulXSS" (hereinafter "PAULXSS"), MIHAI DRAGHICI (hereinafter "M. DRAGHICI"), MARIUS SORIN TOMESCU, aka "Andrei" (hereinafter "TOMESCU"), LUCIAN ZAMFIRACHE, aka Krobelus (hereinafter "ZAMFIRACHE"), LAURENTIU CRISTIAN BUSCA, aka "italianu" (hereinafter "BUSCA"), DAN IONESCU, aka "m1nja" (hereinafter "IONESCU"), OVIDIU-IONUT NICOLA-ROMAN (hereinafter "NICOLA-ROMAN"), MARIUS LNU, aka

"13081981" (hereinafter "MARIUS 13081981"), ALEX GABRIEL PARALESCU, aka "paraiul" (hereinafter "PARALESCU"), FNU LNU, aka "euro_pin_atm" (hereinafter "EURO_PIN_ATM"), ANDREEA NICOLETA STANCUTA, aka "godfather" (hereinafter "STANCUTA"), and others known and unknown to the Grand Jury, conspired and agreed with each other, in violation of Title 18, United States Code, Section 1029(b)(2), to commit the following violations: (1) production, use, and trafficking in counterfeit and unauthorized access devices, in violation of Title 18, United States Code, Section 1029(a)(1); and (2) possession of device-making equipment, in violation of Title 18, United States Code, Section 1029(a)(4).

MEANS BY WHICH THE OBJECTS OF THE CONSPIRACY WERE TO BE ACCOMPLISHED

3. The objects of the conspiracy were to be accomplished in substance as follows:

a. Lee and defendants TRAN, PANAIT, ILINCA, PARVEZ, BULUGEA, N. DRAGHICI, CONSTANTIN, SPIRU, CIULEAN, CRYPTMASTER, SELEQTOR, STANCU, BELBITA, and others known and unknown to the Grand Jury, would create and broadcast spam or SMS text messages, or would cause spam or SMS text messages to be created and broadcast, to holders of bank and credit card accounts, all for the purpose of phishing and smishing, that is, to fraudulently obtain access devices and PII.

b. Defendants PANAIT, ILINCA, PARVEZ, BULUGEA, N. DRAGHICI, CONSTANTIN, SPIRU, CIULEAN, CRYPTMASTER, SELEQTOR, STANCU, BELBITA, PAULXSS, M. DRAGHICI, TOMESCU, ZAMFIRACHE, BUSCA, IONESCU, NICOLA-ROMAN, MARIUS 13081981, PARALESCU,

EURO_PIN_ATM, STANCUTA, and others known and unknown to the Grand Jury (hereinafter collectively, the "supplier defendants"), would supply the results of their and others' fraudulent phishing and smishing attacks to cashiers, including Lee and defendant TRAN, and others known and unknown to the Grand Jury, over the Internet via chat sessions and email.

c. Lee and defendant TRAN would obtain proprietary algorithms, that is, unique numeric codes, for financial institutions and would obtain and use such algorithms and device-making equipment, including computers, encoders, and encoding software, to re-encode access cards, including credit, debit, and gift cards, or hotel keys, with IADs transmitted by the supplier defendants in order to make cashable IADs.

d. Lee and defendants TRAN, SORIANO, GONZALES, NGO, TATH, VO, DANG, PHAN, NGUYEN, LUONG, and others known and unknown to the Grand Jury, would use the cashable IADs to obtain cash, goods, and services, and would wire-transfer proceeds from their fraudulent activity back to the supplier defendants and others known and unknown to the Grand Jury.

OVERT ACTS

The Grand Jury re-alleges and incorporates by reference each of the Overt Acts alleged in Count One as though fully set forth herein, and further alleges that the following overt acts were committed in the Central District of California, and elsewhere:

1. On or about February 28, 2008, defendant NGO caused to be wire transferred via WU the amount of $1,200 to E.A.M. in Romania, which were proceeds from the use of IADs.

2. On or about March 8, 2008, Lee and defendant NGO used IADs to purchase Nordstrom gift cards in a Ralph's Market in Irvine, California.

3. On or about March 4, 2008, defendant NGO caused to be wire transferred via MG the amount of $500 to H.N., which were proceeds from the use of IADs.

4. On or about March 10, 2008, Lee and defendants NGO and SORIANO used room 314 at the Hotel Huntington Beach, Huntington Beach, California, under the name "T.V.," to make IADs.

5. On or about March 14, 2006, defendant TATH withdrew $100 from a Wells Fargo ATM in Seal Beach, California, using an IAD made by defendant TRAN from access device number xxxx-xxxx-xxxx-3285, issued by Southern Lakes Credit Union to N.L.

6. On or about March 14, 2006, defendant TATH attempted to withdraw money from a Wells Fargo ATM in Seal Beach, California, using hotel keys that had been re-encoded with IADs, and which contained a PIN written on a white sticker on the back of each hotel key.

7. On or about August 31, 2007, defendant TATH, at or about the same time as defendants TRAN, LUONG, and PHAN, used an IAD obtained by a phishing attack on E-Trade against account holders S. and. B.C., namely, access device number xxxx-xxxx-xxxx-1231, issued by E-Trade, to purchase goods at Costco in Garden Grove, California.

8. In or about January 2008, defendant TATH used and had the benefit of funds held in Wells Fargo Bank account number xxxxxx9462, in the name of the N.P. Restaurant, into which were

deposited funds from IADs created from access devices and PII acquired in a phishing attack against holders of accounts at the Langley Federal Credit Union.

9. In or about April and May, 2007, Lee and defendant PANAIT and VO met in Orange County, California, to discuss using IADs to withdraw cash from ATMs and POS terminals.

10. In or about April and May, 2007, Lee gave defendant VO several hotel keys that had been re-encoded with IADs obtained from a phishing attack against holders of accounts at E-Trade.

11. Between in or about April and July, 2007, defendant VO obtained approximately $20,000 from ATMs and POS terminals using hotel keys and other access devices that had been re-encoded with IADs obtained from a phishing attack against holders of accounts at E-Trade and other financial institutions.

12. On or about February 5, 2008, Lee and defendant N. DRAGHICI participated in an Internet chat in which Lee stated that he, defendant SORIANO, and defendant DANG would send defendant N. DRAGHICI money via WU.

13. On or about February 5, 2008, Lee and defendants SORIANO and DANG discussed sending money via WU to a supplier of IADs.

14. On or about February 19, 2008, defendant NGO caused to be wire-transferred via MG $200 to H.N., which were proceeds from the use of IADs.

15. On or about August 31, 2007, defendant PHAN, at or about the same time as defendants TRAN, TATH and LUONG, used an IAD obtained by a phishing attack on E-Trade against account

holders S. and B.C., namely, access device number xxxx-xxxx-xxxx-1231, issued by E-Trade, to purchase goods at Costco in Garden Grove, California.

16. On or about February 4, 2008, Lee and defendant PHAN participated in an Internet chat in which Lee asked defendant PHAN to come to Las Vegas to use IADs.

17. In or about February 2008, defendant PHAN met Lee in Las Vegas and withdrew money from ATMs and POS terminals using IADs.

18. In or about January 2007, defendant NGUYEN purchased an MSR encoder for Lee for use in making IADs.

19. In or about May 2007, defendant NGUYEN met with Lee and defendant PANAIT in Las Vegas and discussed IADs.

20. In or about May 2007, defendant NGUYEN on several occasions gave his own debit card to Lee to be re-encoded with IADs, which defendant NGUYEN then used to withdraw cash from ATMs and POS terminals.

21. On or about August 30, 2007, defendant LUONG applied for a Costco membership at Costco in Garden Grove, California.

22. On or about August 31, 2007, defendants LUONG, at or about the same time as defendants TRAN, TATH, and PHAN, used an IAD obtained by a phishing attack on E-Trade against account holders S. and B.C., namely, access device number xxxx-xxxx-xxxx-1231, issued by E-Trade, to purchase goods at Costco in Garden Grove, California.

23. On or about September 20, 2007, defendant LUONG attempted to return for credit at Costco in Garden Grove,

California, a watch he had purchased in the amount of approximately $3,106 on or about August 31, 2007, using an IAD obtained by a phishing attack on E-Trade against account holders S. and B.C.

24. On or about April 30, 2007, Lee and defendant PAULXSS participated in an Internet chat in which defendant PAULXSS told Lee that defendant PAULXSS had sent 80 IADs but some of the PINs did not work.

25. On or about April 30, 2007, Lee and defendant PAULXSS participated in an Internet chat in which they discussed an IAD that had been created from a phishing attack on Keystone Bank.

26. On or about July 23, 2006, defendant TRAN caused to be wire-transferred via WU the amount of $1,500 to defendant TOMESCU in Romania as proceeds from the use of IADs supplied by defendant TOMESCU.

27. On or about March 21, 2007, Lee and defendant TOMESCU participated in an Internet chat in which defendant TOMESCU sent Lee approximately 75 IADs including access device number xxxx-xxxx-xxxx-8160, issued by Iowa League Corporate Central Credit Union.

28. On or about March 12, 2007, defendant BUSCA sent Lee over the Internet approximately 20 IADs including access device number xxxx-xxxx-xxxx-8524, issued by Bank of the West.

29. On or about September 6, 2007, defendant GONZALES, at the direction of Lee, caused to be wire-transferred via WU the amount of $450 to defendant IONESCU in Romania as payment for the supply of IADs.

30. In or about December 2007, Lee spoke over the telephone with defendant IONESCU in Romania regarding a supply of IAD.

31. In or about December 2007 Lee spoke over the telephone with defendant IONESCU in Romania regarding a supply of IAD.

32. On or about December 12, 2007, Lee and defendant IONESCU participated in an Internet chat in which defendant IONESCU sent Lee IADs including access device number xxxx-xxxx-xxxx-0272, issued by Waterbury Teachers' Federal Credit Union.

33. In or about December 2005, defendant TRAN using the name "John Tran," caused to be wire-transferred via VCOM the amount of $921 to defendant NICOLA-ROMAN in Romania as proceeds from the use of IADs.

34. On or about December 2, 2005, defendant TRAN using the name "John Tran," caused to be wire-transferred via VCOM the amount of $140 to defendant NICOLA-ROMAN in Romania as proceeds from the use of IADs.

35. On or about December 4, 2005, defendant TRAN using the name "John Tran," caused to be wire-transferred via MG the amount of $1,000 to defendant NICOLA-ROMAN in Romania as proceeds from the use of IADs.

36. On or about December 8, 2005, defendant TRAN using the name "John Tran," caused to be wire-transferred via MG the amount of $1,900 to defendant NICOLA-ROMAN in Romania as proceeds from the use of IADs.

37. On or about December 9, 2005, defendant TRAN using the name "John Tran," caused to be wire-transferred via VCOM the

amount of $921 to defendant NICOLA-ROMAN in Romania as proceeds from the use of IADs.

38. On or about December 10, 2006, defendant TRAN using the name "John Tran," caused to be wire-transferred via MG the amount of $715 to defendant NICOLA-ROMAN in Romania as proceeds from the use of IADs.

39. On or about December 15, 2006, defendant TRAN, using the name "John Tran," caused to be wire-transferred via MG the amount of $1,705 to defendant NICOLA-ROMAN in Romania as proceeds from the use of IADs.

40. On or about December 22, 2005, defendant TRAN, using the name "John Tran," caused to be wire-transferred via WU the amount of $400 to defendant NICOLA-ROMAN in Romania as proceeds from the use of IADs.

41. On or about December 31, 2005, defendants TRAN and NICOLA-ROMAN participated in an Internet chat during which defendant NICOLA-ROMAN sent defendant TRAN approximately 25 IADs.

42. In or about January 2006, defendant NICOLA-ROMAN accessed from IP addresses assigned to Romania the email collector account entitled, "vercartil@yahoo.com," which then contained access devices and PII obtained by a phishing attack.

43. On or about January 3, 2006, defendant TRAN, using the name "John Tran," caused to be delivered via DHL Express two "refurbished notebook computers" to defendant NICOLA-ROMAN in Romania.

44. On or about February 11, 2006, defendant TRAN, using the name "John Tran," caused to be wire-transferred via MG the

amount of $600 to defendant NICOLA-ROMAN in Romania as proceeds from the use of IADs.

45. In or about March 2006, defendant NICOLA-ROMAN accessed from IP addresses assigned to Romania the email collector account entitled, "fly4hell@yahoo.com," which then contained access devices and PII obtained by a phishing attack.

46. In or about April 2006, defendant NICOLA-ROMAN received an email that contained two Visa credit card numbers with associated Social Security numbers, dates of birth, CVV's, and PINs.

47. On or about July 25, 2007, Lee and defendant MARIUS 13081981 participated in an Internet chat in which defendant MARIUS 13081981 sent Lee approximately seven IADs, including access device number xxxx-xxxx-xxxx-9391, issued by School Financial Credit Union, and related PIN and algorithm.

48. On or about August 4, 2007, Lee and defendant PARALESCU participated in an Internet chat in which defendant PARALESCU sent Lee approximately eight IADs, including access device number xxxx-xxxx-xxxx-7750, issued by Desert Schools Federal Credit Union, and its related PIN and algorithm.

49. On or about August 4, 2007, Lee and defendant EURO_PIN_ATM participated in an Internet chat in which defendant EURO_PIN_ATM sent Lee approximately ten IADs, including access device number xxxx-xxxx-xxxx-8017, issued by Regions Bank, and related PII, account access login codes, and names of account holders for other IADs.

50. On or about April 19, 2007, Lee and defendant STANCUTA

participated in an Internet chat in which defendant STANCUTA sent Lee the first of approximately seven "rounds" of text containing numerous IADs that had been fraudulently obtained from holders of accounts at Washington State Employees Credit Union, including access device number xxxx-xxxx-xxxx-3210, issued by Washington State Employees Credit Union, and related PII.

COUNTS THREE through ELEVEN

[18 U.S.C. §§ 1344(2), 2(a), (b)]

(Bank Fraud and Aiding and Abetting and Causing an Act to be Done)

INTRODUCTORY ALLEGATIONS

1. The Grand Jury realleges and incorporates herein by reference the General Allegations and Definitions of this indictment, as though fully set forth herein.

2. At all times relevant to this indictment, E-Trade was a financial institution whose deposits were federally insured by the Federal Deposit Insurance Corporation.

THE FRAUDULENT SCHEME

3. Beginning at a time unknown and continuing to on or about September 6, 2007, in Los Angeles County and Orange County, within the Central District of California, and elsewhere, Lee and defendants HIEP THANH TRAN, aka John Tran, aka Sam Tran ("TRAN"), SORIN ALIN PANAIT, aka "scumpic4u" ("PANAIT"), LEONARD GONZALES, aka "Bonecrusher" ("GONZALES"), CAROLINE TATH ("TATH"), DUNG PHAN ("PHAN"), and ALEX CHUNG LUONG ("LUONG"), and others known and unknown to the Grand Jury, knowingly, and with intent to defraud, executed and attempted to execute a scheme to obtain monies and funds owned by and in the custody and control of E-Trade by means of material false and fraudulent pretenses, representations, and promises.

4. The fraudulent scheme operated in substance in the following manner:

a. Defendant PANAIT, and others known and unknown to

the Grand Jury, would broadcast or cause to be broadcasted spam, targeting the holders of accounts at financial institutions, including E-Trade, and soliciting the holders of such accounts to log onto an Internet domain, for example, "www.trustworthysite.com," which appeared to be a legitimate site hosted by a financial institution. Once at the site, victims would be prompted to input access device and PII. Defendant PANAIT, and others known and unknown to the Grand Jury, would harvest the information provided by individuals who would respond to the phishing attack and would send the harvested IADs and PII to Lee and other cashiers, including defendant TRAN, over the Internet.

b. Lee and defendant TRAN would obtain and use device-making equipment, including computers, encoders, and access device cards to re-encode access cards with IAD information obtained from defendant PANAIT, and others known and unknown to the Grand Jury, to make cashable IADs.

c. Lee and defendants TRAN, GONZALES, TATH, PHAN, and LUONG, and others known and unknown to the Grand Jury, would use the cashable IADs to obtain cash, goods, and services, and would wire-transfer proceeds from their fraudulent activity to defendant PANAIT.

EXECUTION OF THE FRAUDULENT SCHEME

5. To execute the above-described fraudulent scheme, Lee and defendants, each aiding and abetting the others, committed and attempted to commit, and caused to be committed and attempted to be committed, the following acts, among others, in the Central

District of California, and elsewhere, on or about the below-specified dates, in and affecting interstate commerce, each of which constituted an execution and attempted execution of the fraudulent scheme:

COUNT	DATE	ACT
THREE	8/31/07	Purchase of approximately $3,016.99 in goods from Costco, Garden Grove, California, using E-Trade access device card number xxxx-xxxx-xxxx-1231/3909
FOUR	8/31/07	Purchase of approximately $1,654.55 in goods from Costco, Garden Grove, California, using E-Trade access device card number xxxx-xxxx-xxxx-1231/3909
FIVE	8/31/07	Purchase of approximately $1,292.91 in goods from Costco, Garden Grove, California, using E-Trade access device card number xxxx-xxxx-xxxx-1231/3909
SIX	8/31/07	Purchase of approximately $2,101.11 in goods from Costco, Garden Grove, California, using E-Trade access device card number xxxx-xxxx-xxxx-1231/3909
SEVEN	9/1/07	Purchase of Postal Money Order in the amount of $996.50 at U.S. Postal Service, Buena Park, California, using E-Trade access device card number xxxx-xxxx-xxxx-1231/3909
EIGHT	9/1/07	Purchase of Postal Money Order in the amount of $996.50 at U.S. Postal Service, Buena Park, California, using E-Trade access device card number xxxx-xxxx-xxxx-1231/3909
NINE	9/1/07	Purchase of Postal Money Order in the amount of $1,001.50 at U.S. Postal Service, La Puente, California, using E-Trade access device card number xxxx-xxxx-xxxx-1231/3909

COUNT	DATE	ACT
TEN	9/1/07	Withdrawal in the amount of $1,001.50 at POS terminal, 8215 N.E. Sandy Blvd., Portland, Oregon, using E-Trade access device card number xxxx-xxxx-xxxx-1231/3909
ELEVEN	8/6/07	Withdrawal in the amount of $501.75 at Cardtronics VCOM, 4220 Eagle Rock Blvd., Eagle Rock, California, using E-Trade access device card number xxxx-xxxx-xxxx-1231/3909

COUNTS TWELVE THROUGH FIFTY-SIX

[18 U.S.C. §§ 1029(a)(1), 2(a), 2(b)]

(Production, Use, and Trafficking of Counterfeit Access Devices and Aiding and Abetting and Causing an Act to be Done)

1. The Grand Jury realleges and incorporates herein by reference the General Allegations and Definitions of this indictment, as though fully set forth herein.

2. On or about the dates specified below, in Los Angeles County and Orange County, within the Central District of California, and elsewhere, the defendants named below, in transactions affecting interstate commerce, knowingly and with intent to defraud, produced, used, and trafficked in counterfeit access devices, as follows:

COUNT	DATE	DEFENDANT(S)	COUNTERFEIT ACCESS DEVICE
TWELVE	March 14, 2006	HIEP THANH TRAN, and CAROLINE TATH	Visa debit access card number xxxx-xxxx-xxxx-3285, issued to N.L.
THIRTEEN	March 14, 2006	HIEP THANH TRAN and CAROLINE TATH	Visa debit access card number xxxx-xxxx-xxxx-7311, issued to J.G.
FOURTEEN	March 14, 2006	HIEP THANH TRAN and CAROLINE TATH	Visa debit access card number xxxx-xxxx-xxxx-1960, issued to F.C.
FIFTEEN	March 14, 2006	HIEP THANH TRAN and CAROLINE TATH	Visa debit access card number xxxx-xxxx-xxxx-3758, issued to R.R.

COUNT	DATE	DEFENDANT(S)	COUNTERFEIT ACCESS DEVICE
SIXTEEN	March 14, 2006	HIEP THANH TRAN and CAROLINE TATH	Visa debit access card number xxxx-xxxx-xxxx-7868, issued to D.J.
SEVENTEEN	April 9, 2006	HIEP THANH TRAN and NICOLAE DRAGOS DRAGHICI	access card number xxxx-xxxx-xxxx-2982, issued by Bankers Bank
EIGHTEEN	April 13, 2006	HIEP THANH TRAN and HASSAN PARVEZ	text file on defendant TRAN's computer entitled, "New langley fcu," containing two access device numbers, including xxxx-xxxx-xxxx-2129, issued by Langley Federal Credit Union
NINETEEN	April 13, 2006	HIEP THANH TRAN and HASSAN PARVEZ	access device number xxxx-xxxx-xxxx-2129, issued by Langley Federal Credit Union
TWENTY	August 2, 2006	HIEP THANH TRAN	approximately 100 IADs on TRAN's computer file entitled, "0010.rtf"
TWENTY-ONE	February 26, 2007	FNU LNU, aka "Cryptmaster"	access device number xxxx-xxxx-xxxx-0709, issued by Teacher's Credit Union

COUNT	DATE	DEFENDANT(S)	COUNTERFEIT ACCESS DEVICE
TWENTY-TWO	April 17, 2007	FLORIN GEORGEL SPIRU	access device number xxxx-xxxx-xxxx-2105, issued by Southwest Corporate Federal Credit Union
TWENTY-THREE	April 30, 2007	FNU LNU, aka "Cryptmaster"	access device number xxxx-xxxx-xxxx-6876, issued by Downey Savings & Loan
TWENTY-FOUR	May 2007	FNU LNU, aka "Cryptmaster"	access device number xxxx-xxxx-xxxx-7128, issued by Capital One Bank
TWENTY-FIVE	June 3, 2007	FLORIN GEORGEL SPIRU	access device number xxxx-xxxx-xxxx-7749, issued by Telco Credit Union & Affiliates
TWENTY-SIX	August 22, 2007	IRINEL NICUSOR STANCU	access device number xxxx-xxxx-xxxx-0779, issued by Boeing Employees' Credit Union
TWENTY-SEVEN	November 4, 2007	FLORIN GEORGEL SPIRU	access device number xxxx-xxxx-xxxx-9794, issued by First Merit Bank
TWENTY-EIGHT	May 2, 2007	DIDI GABRIEL CONSTANTIN	access device number xxxx-xxxx-xxxx-7394, issued by Flagstar Bank

COUNT	DATE	DEFENDANT(S)	COUNTERFEIT ACCESS DEVICE
TWENTY-NINE	May 3, 2007	COSTEL BULUGEA	access device number xxxx-xxxx-xxxx-6715, issued by American National Bank of Texas
THIRTY	August 31, 2007	HIEP THANH TRAN, CAROLINE TATH, ALEX CHUNG LUONG, and DUNG PHAN	access device number xxxx-xxxx-xxxx-1231, issued by E-Trade to S. and B.C.
THIRTY-ONE	November 25, 2007	DIDI GABRIEL CONSTANTIN	access device number xxxx-xxxx-xxxx-8431, issued by Premier Credit Union
THIRTY-TWO	January 7, 2008	SORIN ALIN PANAIT	Lee computer text file containing eight (8)access device numbers, including number xxxx-xxxx-xxxx-2470, issued by Jeffco Schools Credit Union
THIRTY-THREE	January 7, 2008	COSTEL BULUGEA	access device numbers xxxx-xxxx-xxxx-6382, issued by Mountain America Credit Union
THIRTY-FOUR	January 8, 2008	COSTEL BULUGEA	access device number xxxx-xxxx-xxxx-2380, issued by Mountain America Credit Union

COUNT	DATE	DEFENDANT(S)	COUNTERFEIT ACCESS DEVICE
THIRTY-FIVE	January 9, 2008	SORIN ALIN PANAIT	Lee computer text file entitled, "2 points," including access device number xxxx-xxxx-xxxx-0731, issued by Pointbank
THIRTY-SIX	January 10, 2008	HASSAN PARVEZ	access device number xxxx-xxxx-xxxx-9217, issued by Capital One Bank
THIRTY-SEVEN	January 10, 2008	HASSAN PARVEZ	access device number xxxx-xxxx-xxxx-9158, issued by Pointbank
THIRTY-EIGHT	January 13, 2008	SORIN ALIN PANAIT	access device number xxxx-xxxx-xxxx-4972, issued by Arizona Federal Credit Union
THIRTY-NINE	January 13, 2008	MARIAN DANIEL CIULEAN	access device number xxxx-xxxx-xxxx-0385, issued by or for the benefit of Payment Systems for Credit Unions, Inc.
FORTY	January 14, 2008	HASSAN PARVEZ	access device numbers xxxx-xxxx-xxxx-2129, issued by Langley Federal Credit Union

COUNT	DATE	DEFENDANT(S)	COUNTERFEIT ACCESS DEVICE
FORTY-ONE	January 16, 2008	HASSAN PARVEZ	access device number xxxx-xxxx-xxxx-4748, issued by Citibank
FORTY-TWO	January 17, 2008	STEFAN SORIN ILINCA	approximately 60 access devices including xxxx-xxxx-xxxx-3662, issued by Artesian City Federal Credit Union
FORTY-THREE	February 1, 2008	NICOLAE DRAGOS DRAGHICI	access device number xxxx-xxxx-xxxx-1468, issued by Pointbank
FORTY-FOUR	February 4, 2008	NICOLAE DRAGOS DRAGHICI	access device number xxxx-xxxx-xxxx-2746, issued by or for the benefit of Payment Systems for Credit Unions, Inc.
FORTY-FIVE	February 10, 2008	PETRU BOGDAN BELBITA	approximately 206 IADs including number xxxx-xxxx-xxxx-5463, issued to S.W.
FORTY-SIX	February 11, 2008	HASSAN PARVEZ and NICOLAE DRAGOS DRAGHICI	access device numbers xxxx-xxxx-xxxx-6897 and xxxx-xxxx-xxxx-0490, issued by Pointbank, and Lee computer text file entitled, "new text document"

COUNT	DATE	DEFENDANT(S)	COUNTERFEIT ACCESS DEVICE
FORTY-SEVEN	February 15, 2008	SORIN ALIN PANAIT	approximately 260 access devices issued by Capital One, including number xxxx-xxxx-xxxx-7694
FORTY-EIGHT	February 15, 2008	HASSAN PARVEZ	approximately 170 access devices, including number xxxx-xxxx-xxxx-3253, issued by Franklin Mint Federal Credit Union
FORTY-NINE	February 17, 2008	MARIAN DANIEL CIULEAN	access device number xxxx-xxxx-xxxx-4386, issued by Langley Federal Credit Union
FIFTY	February 24, 2008	HASSAN PARVEZ	access device number xxxx-xxxx-xxxx-0706, issued by Valley National Bank
FIFTY-ONE	March 10, 2008	MARIAN DANIEL CIULEAN	access device number xxxx-xxxx-xxxx-6938, issued by Allegheny Federal Credit Union
FIFTY-TWO	March 11, 2008	STEFAN SORIN ILINCA	approximately 15 access devices including xxxx-xxxx-xxxx-5971, issued by North Island Credit Union

COUNT	DATE	DEFENDANT(S)	COUNTERFEIT ACCESS DEVICE
FIFTY-THREE	March 11, 2008	STEFAN SORIN ILINCA	North Island Credit Union debit access card number xxxx-xxxx-xxxx-5331, issued to B.T.
FIFTY-FOUR	March 11, 2008	STEFAN SORIN ILINCA and ROLANDO SORIANO	North Island Credit Union debit access card number xxxx-xxxx-xxxx-6310, issued to J.B.
FIFTY-FIVE	March 11, 2008	STEFAN SORIN ILINCA and ROLANDO SORIANO	North Island Credit Union debit access card number xxxx-xxxx-xxxx-0313, issued to D.K.
FIFTY-SIX	March 11, 2008	STEFAN SORIN ILINCA and ROLANDO SORIANO	North Island Credit Union debit access card number xxxx-xxxx-xxxx-2094, issued to V.F.

COUNT FIFTY-SEVEN

[18 U.S.C. § 1029(a)(4)]

(Possession of Device-making Equipment)

On or about August 2, 2006, in Orange County, within the Central District of California, and elsewhere, defendants HIEP THANH TRAN and CAROLINE TATH, knowingly and with intent to defraud, in a transaction affecting interstate and foreign commerce, had custody, control, and possession of device-making equipment, namely, a Dell Inspiron laptop computer, serial number 9CPHF91; a Hewlitt-Packard laptop computer, serial number CND5470C4V; a Logitech flash drive; a Gigatech flash drive; a Lexan flash drive; a Seagate USB hard drive; approximately 22 compact discs; a Fuji compact disc player; a HYTEQ desktop computer; a Western Digital hard drive; an MSR206 card reader; an Operah card printer; an Aurora LM50C card laminator; a Royal Sovereign PRA-5954R laminator; and numerous California driver's license holograms and fraudulent driver's licenses.

COUNTS FIFTY-EIGHT THROUGH FIFTY-NINE

[18 U.S.C. §§ 1030(a)(4), 2(a), 2(b)]

(Accessing Without Authorization and Exceeding Authorized Access of a Protected Computer and Aiding and Abetting and Causing an Act to be Done)

On or about the dates specific below, in Orange County, within the Central District of California, and elsewhere, the defendants named below, knowingly and with the intent to defraud, in transactions affecting interstate and foreign commerce, accessed and exceeded authorized access of the protected computers, specified below, on which was stored financial and credit card information pertaining to access devices, specified below, and by means of such conduct furthered the intended fraud and obtained a thing of value:

COUNT	DATE	DEFENDANT(S)	PROTECTED COMPUTER AND ACCESS DEVICE
FIFTY-EIGHT	March 14, 2006	CAROLINE TATH	Withdrawal from Wells Fargo ATM, connected to Internet, using Visa debit access card number xxxx-xxxx-xxxx-3285, issued to N.L.

COUNT	DATE	DEFENDANT(S)	PROTECTED COMPUTER AND ACCESS DEVICE
FIFTY-NINE	August 31, 2007	HIEP THANH TRAN, CAROLINE TATH, DUNG PHAN, and ALEX CHUNG LUONG	Purchase from Costco, accessing Costco and E-Trade computers connected to Internet from Garden Grove, California, using E-Trade access device number xxxx-xxxx-xxxx-1231/3909, issued to S. and B.C.

COUNTS SIXTY THROUGH SIXTY-FOUR

[18 U.S.C. § 1028A(a)(1)]

(Aggravated Identity Theft)

On or about the dates specified below, in Los Angeles County and Orange County, within the Central District of California, and elsewhere, the defendants named below, in transactions affecting interstate commerce, knowingly and without lawful authority, possessed and used a means of identification of another person, specified below, during and in relation to a felony enumerated in 18 U.S.C. § 1028A(c), namely, fraud and related activity in connection with access devices, in violation of 18 U.S.C. §§ 1029(a)(1), as charged in Counts Twelve through Fifty-Six, and 1029(a)(4), as charged in Count Fifty-Seven as follows:

COUNT	DATE	DEFENDANT(S)	MEANS OF IDENTIFICATION
SIXTY	August 31, 2007	ALEX CHUNG LUONG	access device number xxxx-xxxx-xxxx-xxxx-1231/3909, issued by E-Trade to S. and B.C.
SIXTY-ONE	August 31, 2007	HIEP THANH TRAN	access device number xxxx-xxxx-xxxx-xxxx-1231/3909, issued by E-Trade to S. and B.C.
SIXTY-TWO	August 31, 2007	CAROLINE TATH	access device number xxxx-xxxx-xxxx-xxxx-1231/3909, issued by E-Trade to S. and B.C.

COUNT	DATE	DEFENDANT(S)	MEANS OF IDENTIFICATION
SIXTY-THREE	August 31, 2007	DUNG PHAN	access device number xxxx-xxxx-xxxx-xxxx-1231/3909, issued by E-Trade to S. and B.C.
SIXTY-FOUR	January 18, 2008	HIEP THANH TRAN	access device number xxxx-xxxx-xxxx-xxxx-0732, issued by Langley Federal Credit Union C.S.

COUNT SIXTY-FIVE

[18 U.S.C. § 1963]

1. The General Allegations and Definitions of this indictment, and the allegations contained in Count One of this Indictment, are hereby repeated, realleged, and incorporated by reference herein as though fully set forth at length for the purpose of alleging forfeiture pursuant to the provisions of Title 18, United States Code, Section 1963. Pursuant to Rule 32.2, Fed. R. Crim. P., notice is hereby given to defendants TRAN, PANAIT, ILINCA, PARVEZ, BULUGEA, N. DRAGHICI, CONSTANTIN, SPIRU, CIULEAN, CRYPTMASTER, SELEQTOR, STANCU, and BELBITA that the United States will seek forfeiture as part of any sentence in accordance with Title 18, United States Code, Section 1963 in the event of any defendant's conviction under Count One of this Indictment.

2. Said defendants:

a. Have acquired and maintained interests, in violation of Title 18, United States Code, Section 1962, which interests are subject to forfeiture to the United States pursuant to Title 18, United States Code, Section 1963(a)(1); and

b. Have property constituting and derived from proceeds that they obtained, directly and indirectly, from racketeering activity in violation of Title 18, United States Code, Section 1962, which property is subject to forfeiture to the United States of America pursuant to Title 18, United States Code, Section 1963(a)(3).

3. The interests of the defendants subject to forfeiture

to the United States, pursuant to Title 18, United States Code, Section 1963(a)(1) and (3), include, but are not limited to, at least one million dollars ($1,000,000).

4. If any of the property described herein, as a result of any act or omission of a defendant:

a. Cannot be located upon the exercise of due diligence;

b. Has been transferred or sold to, or disposed 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 that cannot be divided without difficulty;

the Court shall order the forfeiture of any other property of the defendants up to the value of any property set forth above, pursuant to Title 18, United States Code, Section 1963(m).

5. The above-named defendants, and each of them, are

///

///

///

///

///

///

///

///

///

jointly and severally liable for the forfeiture obligations as alleged above.

All pursuant to Title 18, United States Code, Section 1963.

A TRUE BILL

"/S/"

Foreperson

THOMAS P. O'BRIEN
United States Attorney

Christine C Ewell

CHRISTINE C. EWELL
Assistant United States Attorney
Chief, Criminal Division

MICHAEL ZWEIBACK
Assistant United States Attorney
Chief, Cyber & Intellectual Property Crimes Section

WESLEY L. HSU
Assistant United States Attorney
Deputy Chief, Cyber & Intellectual Property Crimes Section

MARK AVEIS
Assistant United States Attorney
Cyber & Intellectual Property Crimes Section