UNITED STATES DISTRICT COURT
DISTRICT OF NEW HAMPSHIRE

UNITED STATES OF AMERICA

v.

ADRIAN-TIBERIU OPREA,
CEZAR IULIAN BUTU,
IULIAN DOLAN, and
FLORIN RADU

Cr. No. 11-cr-64-01/04-SM

INDICTMENT

The Grand Jury charges:

Introduction

At all times material to this Indictment

1. Defendant ADRIAN OPREA, ("OPREA"), also known by online monikers that include "dobitoc212" and "just4you201060," resided in Romania.
2. Defendant CEZAR IULIAN BUTU, aka CEZAR ULIAN BUTI, ("BUTU"), also known by online monikers that include "xjuniior," resided in Romania.
3. Defendant IULIAN DOLAN ("DOLAN"), also known by online monikers that include "iulyvip," "iuly_vip," and "just4you201070," resided in Romania.
4. Defendant FLORIN RADU ("RADU"), also known by online monikers that include "r_florinus," resided in Romania.
5. UNINDICTED CO-CONSPIRATOR ("UC") ONE, also known by the online moniker "tonymontanamiami," resided in an unknown location.

6. UNINDICTED CO-CONSPIRATOR ("UC") TWO, also known by the online moniker "marcos_grande69," resided in an unknown location.

7. From beginning in or before 2008 and continuing through the date of this Indictment, OPREA, BUTU, DOLAN, RADU, UC ONE, UC TWO, and others, conspired to remotely hack into over 200 U.S.-based merchants' point-of-sale ("POS") or "checkout" computer systems in order to steal customers' credit, debit, and gift card numbers and associated data (collectively referred to as "credit card data"). A "POS" system allows merchants to process customer purchases, including those made using credit, debit, and gift card data (collectively referred to as "credit card data"), and typically includes a computer, monitor, integrated credit card processing system, signature capture device, and a customer pin pad device. Merchant victims include more than 150 Subway restaurant franchises located throughout the U.S., including one or more located in the District of New Hampshire, as well as over 50 other identified retailers. Members of the conspiracy have compromised the credit card data of more than 80,000 customers, and millions of dollars of unauthorized purchases have been made using the compromised data.

COUNT ONE
Conspiracy to Commit Computer-Related Fraud
(18 U.S.C. §§ 371 and 1030)

8. Paragraphs 1 through 7 are re-alleged and incorporated as if set forth herein in their entirety.

9. Beginning at a date uncertain, but at least as early as April 2008, and continuing to a date uncertain, but at least as late as March 1, 2011, in the District of New Hampshire and elsewhere, the defendants,

ADRIAN OPREA
CEZAR IULIAN BUTU
IULIAN DOLAN
and
FLORIN RADU

knowingly and intentionally combined, conspired, and agreed together and with each other, and with other persons known and unknown to the Grand Jury, to commit offenses against the United States, namely,

(a) intentionally accessing a computer without authorization and exceeding authorization, and thereby obtaining information contained in a financial record of a financial institution and obtaining information of a card issuer and obtaining information from any protected computer (namely, credit card data), and the offense was committed for purposes of commercial advantage and private financial gain, and was committed in furtherance of any criminal and tortuous act in violation of the Constitution and laws of the United States or of any state; and the value of the information obtained exceeded $5,000, all in violation of 18 U.S.C. §§1030(a)(2)(A)&(C), 1030(c)(2)(B)(i)-(iii);

(b) knowingly, and with intent to defraud, accessing a protected computer without authorization, and exceeding authorized access, and by means of such conduct furthering the intended fraud and obtaining anything of value (namely, credit card data), in violation of 18 U.S.C. §1030(a)(4);

(c) knowingly causing the transmission of a program, information, code, and command, and as a result of such conduct, intentionally causing damage without authorization, to a protected computer, in violation of 18 U.S.C. §1030(a)(5)(A).

Object of the Conspiracy

10. It was the object of the conspiracy for OPREA, BUTU, DOLAN, RADU, UC ONE, UC TWO, and others to hack into and install software code on merchant victims' POS systems in order to steal credit card data from those systems, which information was used to make unauthorized charges and/or was sold to others to reap profits for the co-conspirators.

Manner and Means of the Conspiracy

11. It was part of the conspiracy that members remotely scanned the internet to identify vulnerable POS systems with certain remote desktop software applications ("RDAs") installed on them, and using these RDAs, the conspirators logged onto the targeted POS systems over the internet, either by guessing the passwords or using password-cracking software programs.

12. It was further part of the conspiracy that members remotely and surreptitiously installed software programs called "keystroke loggers" (or "sniffers") onto the POS systems, which would record and store data that was keyed into or swiped through the merchants' POS systems, including customers' credit card data.

13. It was further part of the conspiracy that members often installed a "back door Trojan" into the POS systems that would allow the conspirators to access the compromised POS systems in the future in order to install or re-install additional software programs (collectively referred to as "hacker tools") that facilitated their POS-hacking scheme. The conspirators repeatedly downloaded a hacker tool that is designed to evade detection, "xp.exe," from the "kitsite.info" "dump site" onto victims' POS terminals.

14. It was further part of the conspiracy that, once the keystroke loggers recorded and stored the credit card data from the compromised POS systems, the conspirators caused the data to be

electronically transferred or "uploaded" over the internet to several computer servers, or "dump sites."

15. It was further part of the conspiracy that, at the outset of and throughout the conspiracy, the conspirators set up several U.S.-based internet-connected computers for use as data storage "dump sites." These "dump sites" included the following: "ftp.shopings.info," "ftp.justfuckit.info," "ftp.cindarella.info," "ftp.kitsite.info," "ftp.tushtime.info," and "ftp.canadasite.info." The "dump sites" also included compromised internet-connected computers belonging to unsuspecting small business owners or individuals, including a computer server owned by a small business in Pennsylvania ("the compromised Pennsylvania server").

16. It was further part of the conspiracy that members electronically transferred (or "exfiltrated") the stolen credit card data from the U.S. "dump sites" to overseas computer servers that they controlled, including a site hosted by a webhosting company called "sendspace.com" ("the sendspace.com site").

17. It was further part of the conspiracy that members "monetized" their stolen credit card data by making unauthorized charges on the compromised accounts or by re-selling or otherwise transferring the stolen credit card data to others to do the same.

18. It was further part of the conspiracy that members created phony plastic credit cards by using hardware and software devices (including magnetic stripe readers/writers) to encode blank plastic cards with the stolen credit card data. They then used these encoded plastic cards to make unauthorized charges with various merchants, primarily located throughout Europe.

19. It was further part of the conspiracy that members would also sell or otherwise transfer the stolen credit card data to others by providing them with access to the "sendspace.com" server.

20. It was further part of the conspiracy that members attempted to conceal their identities by, among other things, (1) using stolen identities and credit card numbers to acquire the "dump sites," the various e-mail and instant messaging ("IM") accounts, and the keystroke loggers; (2) issuing "delete" commands to delete any traces of their activities from the "dump sites"; (3) disguising their own computer's Internet Protocol address by using "proxy" computers; (4) communicating with one another over the internet using IM and multiple, frequently changing screen names and e-mail addresses; and (5) using untraceable disposable accounts with Romanian ISPs to access the internet from Romania.

Overt Acts

Hacking into Merchants' POS Systems and Sharing Hacker Tools

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

    a. On or before May 2009, members of the conspiracy made unauthorized access to a POS system located at a Subway franchise restaurant in Plaistow, New Hampshire, and installed a keystroke logger.

    b. On or about December 11, 2009, members of the conspiracy made unauthorized access to a POS system located at a Subway franchise restaurant in East Northport, New York, and installed a keystroke logger.

c. On or about January 7, 2010, members of the conspiracy made unauthorized access to a POS system located at a Subway franchise restaurant in Ocala, Florida, and installed a keystroke logger.

d. On or about March 3, 2010-April 12, 2010, members of the conspiracy made unauthorized access to a POS system located at a Subway franchise restaurant in Fairborn, Ohio, and installed a keystroke logger.

e. On or about April 16, 2010, members of the conspiracy made an online purchase, using a stolen credit card and identity, of a keystroke logger, and made unauthorized access to a POS system located at a Subway franchise restaurant in Tulare, California, and installed the keystroke logger on it.

f. On November 2, 2010, DOLAN sent an e-mail message that contained an attachment, titled "xp.exe," which is an executable file frequently used in computer hacking schemes to avoid detection.

g. A few hours earlier on November 2, 2010, RADU had sent to DOLAN an e-mail message that contained that same "xp.exe" attachment.

Setting Up "Dump Sites"

h. From in or about April 2008 through February 2010, members of the conspiracy, using stolen identification and stolen credit card data, opened multiple accounts at a U.S. webhosting company, GoDaddy, Inc., to create "dump sites" to store the stolen credit card data that was transferred via FTP from the compromised POS systems.

i. On April 4, 2008, members of the conspiracy set up a "dump site" called "ftp.justfuckit.info."

j. On or about April 18, 2008, members of the conspiracy set up a "dump site" called "ftp.tushtime.info."

k. On or about December 18, 2009, members of the conspiracy set up a "dump site" called "ftp.shopings.info."

l. On or about February 14, 2010, members of the conspiracy set up a "dump site" called "ftp.cindarella.info."

m. On or about February 14, 2010, members of the conspiracy set up a "dump site" called "ftp.kitsite.info."

n. On or about February 15, 2010, members of the conspiracy set up a "dump site" called "ftp.canadasite.info."

o. On or about May 14, 2010, DOLAN sent an e-mail message to himself containing the username and password, as well as the web address, "ftp.canadasite.info," to access that "dump site."

p. On or before June 21, 2010, members of the conspiracy made unauthorized access to a computer server belonging to a small business, located in Mechanicsburg, Pennsylvania, and set it up as a "dump site."

Transferring Stolen Credit Card Data From Merchant POS Systems to "Dump Sites"

q. In or about May 2009 through February 2010, members of the conspiracy caused stolen credit card data to be transferred from a Subway restaurant's POS system located in Plaistow, New Hampshire, to the ftp.tushtime.info "dump site."

r. In or about December 11, 2009 through April 17, 2010, members of the conspiracy caused stolen credit card data to be transferred from a Subway restaurant's POS system located in East Northport, New York, to the ftp.justfuckit.info "dump site."

s. In or about January 7, 2010 through March 9, 2010, members of the conspiracy caused stolen credit card data to be transferred from a Subway restaurant's POS system located in Ocala, Florida, to the ftp.shopings.info "dump site."

t. In or about March 3, 2010 through April 12, 2010, members of the conspiracy caused stolen credit card data to be transferred from a Subway restaurant's POS system located in Fairborn, Ohio, to the ftp.cindarella.info "dump site."

u. In or about July 6, 2010 through at least November 22, 2010, members of the conspiracy transferred stolen credit card data from the canadasite.info and cindarella.info "dump sites" to the compromised Pennsylvania server.

Transferring Stolen Credit Card Data
From "Dump Sites" To Co-Conspirators Overseas

v. On or about October, 28, 2010, OPREA accessed the compromised Pennsylvania "dump site" and exfiltrated a file containing stolen credit, debit, and /or gift card numbers and associated data ("credit card data"), transferring it to a server located at "sendspace.com."

w. On or about October 28, 2010, OPREA, during an online chat with BUTU, agreed to sell BUTU credit card data. OPREA provided BUTU with a hyperlink to the "sendspace.com" website, where the stolen credit card data was stored. In that chat, BUTU asked OPREA, "those 70 that you gave me, were they debit cards or credit cards" and OPREA responded: "it was an entire store." OPREA then instructed

BUTU to "send money via western union to someone at home to wire it to me at a raiffesen bank account."

Monetizing Through Creating Phony Credit Cards, Making Unauthorized Charges and/or Transferring Stolen Data to Co-Conspirators

x. On February 16, 2010, BUTU attempted to purchase an embossing machine, which is a hardware device that is commonly used in credit card theft schemes and enables stolen credit card data to be typed or "embossed" onto a blank plastic card in order to create phony credit, debit, or gift cards.

y. On or about October 28, 2010, BUTU, during an online chat with OPREA, told OPREA that he was in France, and had rented a house close by in Belgium, with a group of others, using his "machines" to create phony plastic credit cards from credit card data, that he was using those phony cards to, among other uses, place bets at local French "tobacco" shops, and that he needed more card data from OPREA that had higher dollar limits.

z. On or about November 7, 2010, two unauthorized purchases were made from one of the compromised accounts discussed during the October 28 online chat at a merchant in France.

aa. On or about January 14, 2011, DOLAN sent himself an e-mail message with an attachment that contained four text files, each of which contained hundreds of card numbers and associated data.

bb. A few hours later, on January 14, 2011, DOLAN sent OPREA an e-mail message that contained the same attachment that DOLAN had sent to himself. The text of the e-mail, which was written in Romanian, translated to: "See that's that big shop in 2 fils

splituit 212 and 214 . . . like these are made from the terminals coming . . . . Let me say if these are good on this big shop . . . so if they come and there are many good . . . . maybe we can do something."

cc. On or before January 2011, an unidentified Romanian individual obtained from OPREA a list of 38 American Express payment card numbers that corresponded to card numbers that were compromised at six Subway locations, including the Subway in Plaistow, New Hampshire.

All in violation of Title 18, United States Code, Sections 371 and 1030.

COUNT TWO
Conspiracy to Commit Wire Fraud
(18 U.S.C. §§ 1343 and 1349)

22. The allegations set forth in paragraphs 1 through 7 and 11 through 21 of Count One of the Indictment are re-alleged and incorporated as set forth herein.

23. Beginning in or about April 2008, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, but at least as late as May 1, 2011, in the District of New Hampshire and elsewhere, the defendants

ADRIAN OPREA
CEZAR IULIAN BUTU
IULIAN DOLAN
and
FLORIN RADU

knowingly and intentionally combined, conspired, and agreed together and with each other, and with other persons known and unknown to the Grand Jury, to commit offenses against the United States, namely, to devise a scheme and artifice to defraud the merchant victims, their customer cardholders, and the financial institutions that issued credit, debit, and gift cards to those customers, and to obtain money and property, by means of materially false and fraudulent pretenses, representations, and promises, and for the purpose of executing the scheme and artifice to defraud, transmitted and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, in violation of Title 18, United States Code, Sections 1343 and 1349.

Object of the Conspiracy

24. It was the object of the conspiracy for defendants OPREA, BUTU, DOLAN, RADU, UC ONE, UC TWO, and others to reap profits by defrauding merchants, cardholders, and card issuers by making unauthorized charges and re-selling credit card numbers and corresponding card data that had been stolen from merchants' compromised POS systems.

Manner and Means of the Conspiracy

25. It was part of the conspiracy that, once members of the conspiracy had stolen credit card numbers and corresponding card data from the victim merchants' compromised POS systems, members would use the stolen card data to make unauthorized charges on the accounts and would sell or otherwise distribute the stolen card data to others to make unauthorized charges.

26. It was further part of the conspiracy that those who purchased batches of the stolen card data would further distribute the data to others, where it would be used to make unauthorized purchases at retail locations, gambling institutions, to make unauthorized withdrawals from banks and financial institutions, and to further identity theft schemes.

Overt Acts

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

    a. On or before May 2009, members of the conspiracy made unauthorized access to a POS system located at a Subway franchise restaurant in Plaistow, New Hampshire, and installed a keystroke logger.

    b. On or about October 28, 2010, OPREA accessed the compromised Pennsylvania server and exfiltrated a file containing stolen credit card data, transferring it to a server located at "sendspace.com," which American Express and Citibank have verified were authentic access devices that were unauthorized (they were credit card account numbers that were issued to other persons that had been stolen, lost, expired, revoked, canceled or obtained with intent to defraud).

c. On or about October 28, 2010, during an online chat, OPREA agreed to sell BUTU stolen credit card data and then transferred the data by providing BUTU with a link to a website at "sendspace.com" where the data was stored.

d. Or about November 7, 2010, two unauthorized purchases were made from one of the compromised accounts at a merchant located in France.

e. On or about January 14, 2011, DOLAN sent OPREA an e-mail message with an attatchment containing hundreds of stolen credit card numbers and associated credit card data.

All in violation of Title 18, United States Code, Sections 1343 and 1349.

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

28. The allegations set forth in paragraphs 1 through 7 and 11 through 21 of Count One and paragraphs 25 through 27 of Count Two of the Indictment are re-alleged and incorporated as set forth herein.

29. Beginning at a date uncertain, but at least as early as May 2009, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, but at least as late as March 1, 2011, in the District of New Hampshire and elsewhere, the defendants

ADRIAN OPREA
CEZAR IULIAN BUTU
IULIAN DOLAN
and
FLORIN RADU

knowingly and with intent to further the object of the conspiracy combine, conspire, confederate and agree with each other and with persons known and unknown to the Grand Jury, to commit an offense under Title 18, United States Code, Section 1029(a), specifically, to knowingly and with intent to defraud traffic in and use one or more unauthorized access devices during any one-year period, that is, unauthorized access device numbers and corresponding data, and by such conduct obtain anything of value aggregating $1,000 or more during that period, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(2).

Object of the Conspiracy

30. It was the object of the conspiracy for defendants OPREA, BUTU, DOLAN, RADU, UC ONE, UC TWO, and others to profit from (a) acquiring access device numbers and corresponding data from co-conspirators or victim merchants, knowing that the numbers had been stolen; and (b) selling those access device numbers and corresponding data to other co-

conspirators, knowing that the access device numbers and corresponding data would be used for the personal use and benefit of co-conspirators, without the knowledge or consent of the true account holders.

Manner and Means of the Conspiracy

31. It was part of the conspiracy that OPREA contacted co-conspirators via the Internet and acquired access device information in bulk, including unauthorized access device numbers and corresponding data, which OPREA knew to be stolen. OPREA acquired over 15 access device numbers and corresponding data in this manner.

32. It was further part of the conspiracy that OPREA sold or otherwise transferred the stolen access device information to other co-conspirators, including BUTU, knowing they would use the information to make fraudulent purchases without authorization from the true account holders.

33. It was further part of the conspiracy that BUTU contacted co-conspirators, including OPREA, and purchased or otherwise acquired access device information in bulk, including unauthorized access device numbers and corresponding data, which BUTU knew to be stolen. BUTU acquired at least 15 unauthorized access device numbers and corresponding data in this manner.

34. It was further part of the conspiracy that BUTU further used the stolen access device information to unlawfully manufacture access devices without authorization from the true access device account holders or the access device issuers.

Overt Acts

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

    a. On or before May 2009, members made unauthorized access to a POS system located at a Subway franchise restaurant in Plaistow, New Hampshire, and installed a keystroke logger.

    b. On or about October 28, 2010, OPREA accessed the compromised Pennsylvania server and exfiltrated a file containing stolen credit card data, transferring it to a server located at "sendspace.com."

    c. On or about October 28, 2010, during an online chat, OPREA agreed to sell BUTU stolen credit card data and then transferred the data by providing BUTU with a link to a website at "sendspace.com" where the data was stored.

    d. Or about November 7, 2010, two unauthorized purchases were made from one of the compromised accounts at a merchant located in France.

    e. On or about January 14, 2011, DOLAN sent OPREA an e-mail message with an attachment containing hundreds of stolen access device numbers and associated credit card data.

    All in violation of Title 18, United States Code, Section 1029(a)(3).

COUNT FOUR
Conspiracy to Commit Fraud in Connection with Access Devices
(18 U.S.C. § 1029(a)(3))

36. The allegations set forth in paragraphs1 through 7 and 11 through 21 of Count One, paragraphs 25 through 27 of Count Two, and paragraphs 31 through 35 of Count Three of the Indictment are re-alleged and incorporated as set forth herein.

37. Beginning at a date uncertain, but at least as early as May 2009, the exact date being unknown to the Grand Jury, and continuing to a date uncertain, but at least as late as March 1, 2011, in the District of New Hampshire and elsewhere, the defendants

ADRIAN OPREA
CEZAR IULIAN BUTU
IULIAN DOLAN
and
FLORIN RADU

knowingly and with intent to further the object of the conspiracy combine, conspire, confederate and agree with each other and with persons known and unknown to the Grand Jury, to commit an offense under Title 18, United States Code, Section 1029(a), specifically, to knowingly and with intent to defraud possess fifteen or more unauthorized access devices, said conduct affecting interstate and foreign commerce, in violation of Title 18, United States Code, Section 1029(a)(3).

Object of the Conspiracy

38. It was the object of the conspiracy for defendants OPREA, BUTU, DOLAN, RADU, UC ONE, UC TWO, and others to profit from (a) acquiring access device numbers and corresponding data from co-conspirators or victim merchants, knowing that the numbers had been stolen; and (b) selling those access device numbers and corresponding data to other co-conspirators, knowing that the access device numbers and corresponding data would be used

for the personal use and benefit of co-conspirators, without the knowledge or consent of the true account holders.

Manner and Means of the Conspiracy

39. It was part of the conspiracy that OPREA contacted co-conspirators via the Internet and acquired access device information in bulk, including unauthorized access device numbers and corresponding data, which OPREA knew to be stolen. OPREA acquired over 15 access device numbers and corresponding data in this manner.

40. It was further part of the conspiracy that OPREA sold or otherwise transferred the stolen access device information to other co-conspirators, including BUTU, knowing they would use the information to make fraudulent purchases without authorization from the true account holders.

41. It was further part of the conspiracy that BUTU contacted co-conspirators, including OPREA, and purchased or otherwise acquired access device information in bulk, including unauthorized access device numbers and corresponding data, which BUTU knew to be stolen. BUTU acquired at least 15 unauthorized access device numbers and corresponding data in this manner.

42. It was further part of the conspiracy that BUTU further used the stolen access device information to unlawfully manufacture access devices without authorization from the true access device account holders or the access device issuers.

Overt Acts

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

a. On or before May 2009, members made unauthorized access to a POS system located at a Subway franchise restaurant in Plaistow, New Hampshire, and installed a keystroke logger.

b. On or about October 28, 2010, OPREA accessed the compromised Pennsylvania server and exfiltrated a file containing stolen credit card data, transferring it to a server located at "sendspace.com."

c. On or about October 28, 2010, during an online chat, OPREA agreed to sell BUTU stolen credit card data and then transferred the data by providing BUTU with a link to a website at "sendspace.com" where the data was stored.

d. Or about November 7, 2010, two unauthorized purchases were made from one of the compromised accounts at a merchant located in France.

e. On or about January 14, 2011, DOLAN sent OPREA an e-mail message with an attachment containing hundreds of stolen access device numbers and associated credit card data.

All in violation of Title 18, United States Code, Section 1029(a)(3).

May 4, 2011

TRUE BILL

/s/ Foreperson
Grand Jury Foreperson

John P. Kacavas
United States Attorney

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

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