EXHIBIT 2

FILED
IN CLERK'S OFFICE
U.S. DISTRICT COURT E.D.N.Y.

★ MAY 14 2008 ★

LONG ISLAND OFFICE

RPD:KKP:ECW
F. #2007R01826

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- X

UNITED STATES OF AMERICA

- against -

MAKSYM YASTREMSKIY,
also known as "Maksik,"
ALEKSANDR SUVOROV,
also known as "JonnyHell," and
ALBERT GONZALEZ,
also known as "Segvec,"

Defendants.

- X

S U P E R S E D I N G
I N D I C T M E N T

Cr. No. 08-160(S-1)(SJF)
(T. 18, U.S.C., §§ 371, 981(a)(1)(C), 982(a)(2)(B), 1028A(a)(1), 1028A(b), 1028A(c)(5), 1029(a)(3), 1029(b)(2), 1029(c)(1)(A)(i), 1030(a)(2)(C), 1030(a)(4), 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(c)(2)(B)(i), 1030(c)(3)(A), 1030(c)(4)(A), 1343, 1349, 2511(1)(a), 2511(4)(a), 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

THE GRAND JURY CHARGES:

INTRODUCTION

At all times relevant to this Indictment, unless otherwise indicated:

The Victim Entity

1. Dave & Buster's, Inc. ("D&B") was a Missouri corporation with its corporate headquarters in Dallas, Texas. D&B was a national restaurant chain with 49 locations nationwide. Each D&B restaurant offered its customers full-service dining, a

video arcade and other games. A D&B restaurant was located in Islandia, New York, which was known within D&B as "Store #32" ("D&B Store #32").

2. Each D&B restaurant maintained, operated and used what was known as a "point-of-sale" ("POS") system for processing credit and debit card transactions. Among other things, D&B used the POS system to verify the validity of credit and debit card numbers.

3. The POS system in each D&B restaurant included several components, which were all connected to a central computer system known as the POS "server." The POS system's process included four steps. First, the credit or debit card was swiped at a POS "terminal," which was a magnetic card reader located next to a cash register. Second, certain information from the credit or debit card -- such as the account number, expiration date, security code and discretionary institution data, known collectively as "Track 2" data because it was all contained in the second of two "tracks" inside a magnetic stripe on the back of a credit or debit card -- was transmitted from the POS terminal to the D&B restaurant's POS server. Third, the Track 2 data was transmitted from the POS server through computer systems at D&B's corporate headquarters to the computer systems of a "data processor," a third party which performed the account number verification process on behalf of merchants and other

parties that accepted credit and debit cards as payments. Finally, the data processor transmitted information back through computer systems at D&B's corporate headquarters to the POS server either approving or denying the credit or debit card transaction request.

THE SCHEME TO DEFRAUD

4. From in and around April 2007 to on or about September 22, 2007, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," did devise, and intend to devise, a scheme and artifice to defraud and to obtain money and property by means of materially false and fraudulent pretenses, representations and promises, by remotely accessing, without authorization, POS servers at D&B restaurants in order to acquire Track 2 data that they could sell to others who, in turn, would use the data to make fraudulent purchases or re-sell it to others to make such purchases, causing losses to financial institutions, as set forth in more detail below.

5. In or about April 2007, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ, using interstate and international computer transmissions, gained unauthorized access to the POS server in a D&B restaurant located in Arundel, Maryland and installed a "packet sniffer," which was a malicious computer program comprised of a piece of computer

code designed to capture communications between two or more computer systems on a single network. In order to gain access to the POS server, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ made materially false representations indicating that they were authorized to gain such access. The packet sniffer installed by the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ was configured to capture Track 2 data as it moved from the restaurant's POS server through the computer system at D&B's corporate headquarters to the data processor's computer system. The packet sniffer malfunctioned, however, and the defendants YASTREMSKIY, SUVOROV and GONZALEZ did not capture any Track 2 data.

6. In or about May 2007, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ, using interstate and international computer transmissions, gained unauthorized access to the POS servers in 11 D&B restaurants located in various places in the United States (the "compromised D&B POS servers") and installed packet sniffers at each restaurant. In order to gain access to the POS servers, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ made materially false representations indicating that they were authorized to gain such access. The packet sniffers functioned correctly this time and captured Track 2 data moving from the compromised D&B POS servers to the computer systems at

D&B corporate headquarters to the data processor's computer system. At each D&B restaurant, the packet sniffer created a computer file for individual credit or debit card transactions entitled "log" to store the Track 2 data captured from the packet sniffer. The log file continued to capture Track 2 data until the file was collected by the defendants, at which time the packet sniffer would create a new log file.

7. In addition, as a result of a defect in the software program for the packet sniffer, the packet sniffer automatically deactivated whenever the compromised D&B POS servers rebooted in the normal course of the operation of the servers. Therefore, in order for the packet sniffers to capture data from the compromised D&B POS servers on an ongoing basis, the defendants YASTREMSKIY, SUVOROV and GONZALEZ had to regularly reactivate the packet sniffers.

8. In or about and between May 2007 and September 2007, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ gained unauthorized access to the compromised D&B POS servers, collected the Track 2 data stored in the "log" files in the servers, and reactivated the packet sniffers which were installed on the compromised D&B POS servers.

Intrusions at D&B Store #32

9. On or about May 18, 2007, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ, using

interstate and international computer transmissions, gained unauthorized access to the POS server at D&B Store #32 and installed a packet sniffer designed to capture Track 2 data moving from the POS server through the computer system at the corporate headquarters to the data processor's computer system.

10. On or about June 9, 2007, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ, using interstate and international computer transmissions, gained unauthorized access to the POS server at D&B Store #32, collected a log file and reactivated the packet sniffer.

11. On or about July 23, 2007, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ, using interstate and international computer transmissions, gained unauthorized access to the POS server at D&B Store #32, collected a log file and reactivated the packet sniffer.

12. On or about August 14, 2007, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ, using interstate and international computer transmissions, gained unauthorized access to the POS server at D&B Store #32, collected a log file, and reactivated the packet sniffer.

13. On or about September 22, 2007, the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ, using interstate and international computer transmissions, gained unauthorized access to the POS server at D&B Store #32 and

attempted to retrieve a log file and reactivate the packet sniffer.

14. The log files that the defendants MAKSYM YASTREMSKIY, ALEKSANDR SUVOROV and ALBERT GONZALEZ retrieved from D&B Store #32 contained Track 2 data for approximately 5,000 credit and debit cards. YASTREMSKIY, SUVOROV, GONZALEZ and others then sold the Track 2 data to others who, in turn, used the data to make fraudulent purchases at various retail locations and from various online merchants, causing losses of at least $600,000 to the financial institutions that issued the credit and debit cards.

COUNT ONE
(Conspiracy to Commit Wire Fraud)

15. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

16. On or about and between April 30, 2007 and September 22, 2007, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud D&B, its customers and the financial institutions that issued the customers' credit and debit cards, and to obtain money and

property from D&B, its customers and the financial institutions that issued the customers' credit and debit cards, by means of materially false and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, in violation of Title 18, United States Code, Section 1343.

(Title 18, United States Code, Sections 1349 and 3551 et seq.)

COUNTS TWO THROUGH FIVE
(Wire Fraud)

17. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

18. On or about the dates set forth below, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and intentionally devise a scheme and artifice to defraud D&B, its customers and the financial institutions that issued the customers' credit and debit cards, and to obtain money and property from D&B, its customers and the financial institutions that issued the customers' credit and debit cards, by means of materially false

and fraudulent pretenses, representations and promises, and for the purpose of executing such scheme and artifice, and attempting to do so, transmitted and caused to be transmitted, by means of wire communication in interstate and foreign commerce, writings, signs, signals, pictures and sounds, to wit: the computer transmissions set forth below:

COUNT	DATE	INTERSTATE WIRE COMMUNICATION
2	5/18/07	Packet sniffer installed on POS server at D&B Store #32 in Islandia, New York.
3	6/9/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York.
4	7/23/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York.
5	8/14/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York.

(Title 18, United States Code, Sections 1343, 2 and 3551 et seq.)

COUNT SIX

(Conspiracy to Possess Unauthorized Access Devices)

19. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

20. On or about and between April 30, 2007 and September 22, 2007, both dates being approximate and inclusive,

within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and with intent to defraud conspire to possess fifteen or more unauthorized access devices, to wit: credit card and debit card account numbers, in a manner affecting interstate commerce, in violation of Title 18, United States Code, Section 1029(a)(3).

21. In furtherance of the conspiracy and to effect its objectives, the defendants YASTREMSKIY, SUVOROV, GONZALEZ and others committed and caused to be committed, among others, the following:

OVERT ACTS

a. On or about May 18, 2007, YASTREMSKIY, SUVOROV and GONZALEZ gained unauthorized access to the POS server at D&B Store #32 and installed a packet sniffer.

b. On or about June 9, 2007, YASTREMSKIY, SUVOROV and GONZALEZ gained unauthorized access to the POS server at D&B Store #32, collected a log file and reactivated the packet sniffer.

c. On or about July 23, 2007, YASTREMSKIY, SUVOROV and GONZALEZ gained unauthorized access to the POS server at D&B Store #32, collected a log file and reactivated the packet

sniffer.

(Title 18, United States Code, Sections 1029(b)(2), 1029(c)(1)(A)(i) and 3551 et seq.)

COUNTS SEVEN THROUGH NINE
(Possession of Unauthorized Access Devices)

22. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

23. On or about the dates set forth below, within the Eastern of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and with intent to defraud possess fifteen or more unauthorized access devices, in a manner affecting interstate commerce, as set forth below:

COUNT	DATES	POSSESSION
7	5/18/07 - 6/6/07	Log file containing 15 or more credit and debit card account numbers created by packet sniffer on POS server at D&B Store #32 in Islandia, New York.
8	6/9/07 - 6/28/07	Log file containing 15 or more credit and debit card account numbers created by packet sniffer on POS server at D&B Store #32 in Islandia, New York.
9	7/23/07 - 7/25/07	Log file containing 15 or more credit and debit account card numbers created by packet sniffer on POS server at D&B Store #32 in Islandia, New York.

(Title 18, United States Code, Sections 1029(a)(3), 1029(c)(1)(A)(i), 2 and 3551 et seq.)

COUNT TEN
(Aggravated Identity Theft)

24. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

25. On or about June 9, 2007, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, during and in relation to the crime charged in Count Three, did knowingly and intentionally possess, without lawful authority, means of identification of

other persons, to wit: credit and debit card account numbers of individuals.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(5), 2 and 3551 et seq.)

COUNT ELEVEN
(Aggravated Identity Theft)

26. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

27. On or about July 23, 2007, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, during and in relation to the crime charged in Count Four, did knowingly and intentionally possess, without lawful authority, means of identification of other persons, to wit: credit and debit card account numbers of individuals.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(5), 2 and 3551 et seq.)

COUNT TWELVE
(Aggravated Identity Theft)

28. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

29. On or about August 14, 2007, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, during and in relation to the crime charged in Count Five, did knowingly and intentionally possess, without lawful authority, means of identification of other persons, to wit: credit and debit card account numbers of individuals.

(Title 18, United States Code, Sections 1028A(a)(1), 1028A(b), 1028A(c)(5), 2 and 3551 et seq.)

COUNT THIRTEEN
(Conspiracy to Commit Computer Fraud)

30. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

31. On or about and between April 30, 2007 and September 22, 2007, both dates being approximate and inclusive, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and willfully conspire to: (a) intentionally access a computer without authorization, and thereby obtain information from a protected computer, to wit: credit and debit card account

numbers, in a manner that involved interstate and foreign communications, in violation of Title 18, United States Code, Section 1030(a)(2)(C); (b) knowingly and with intent to defraud access a protected computer without authorization, and by means of such conduct to further the intended fraud and obtain things of value, to wit: credit and debit card account numbers, in violation of Title 18, United States Code, Section 1030(a)(4); and (c) knowingly cause the transmission of a program, information, code and command, and as a result of such conduct, to intentionally cause damage without authorization to a protected computer, to wit: installation of a packet sniffer on the compromised D&B POS servers, in violation of Title 18, United States Code, Section 1030(a)(5)(A)(i).

32. In furtherance of the conspiracy and to effect its objectives, the defendants YASTREMSKIY, SUVOROV, GONZALEZ and others committed and caused to be committed, among others, the following:

OVERT ACTS

a. On or about May 18, 2007, YASTREMSKIY, SUVOROV and GONZALEZ gained unauthorized access to the POS server at D&B Store #32 and installed a packet sniffer.

b. On or about June 9, 2007, YASTREMSKIY, SUVOROV and GONZALEZ gained unauthorized access to the POS server at D&B Store #32, collected a log file and reactivated the packet

sniffer.

c. On or about July 23, 2007, YASTREMSKIY, SUVOROV and GONZALEZ gained unauthorized access to the POS server at D&B Store #32, collected a log file and reactivated the packet sniffer.

(Title 18, United States Code, Sections 371 and 3551 et seq.)

COUNTS FOURTEEN THROUGH SIXTEEN
(Unauthorized Computer Access
Involving an Interstate Communication)

33. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

34. On or about the dates set forth below, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and intentionally access a computer without authorization, and did thereby obtain information from a protected computer, to wit: credit and debit card account numbers, in a manner that involved interstate and foreign communications, which offense was committed for purposes of commercial advantage and private financial gain, to wit: profiting from selling stolen credit and debit card account numbers, as set forth below:

COUNT	DATE	UNAUTHORIZED ACCESS
14	6/9/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York and log file collected.
15	7/23/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York and log file collected.
16	8/14/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York and log file collected.

(Title 18, United States Code, Sections 1030(a)(2)(C), 1030(c)(2)(B)(i), 2 and 3551 et seq.)

COUNTS SEVENTEEN THROUGH NINETEEN
(Unauthorized Computer Access to Obtain Things of Value)

35. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

36. On or about the dates set forth below, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and with intent to defraud access a protected computer without authorization, and by means of such conduct furthered the intended fraud and obtained

things of value, to wit: credit and debit card account numbers, as set forth below:

COUNT	DATE	UNAUTHORIZED ACCESS
17	6/9/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York and log file collected.
18	7/23/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York and log file collected.
19	8/14/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York and log file collected.

(Title 18, United States Code, Sections 1030(a)(4), 1030(c)(3)(A), 2 and 3551 et seq.)

COUNTS TWENTY THROUGH TWENTY-THREE
(Unlawful Transmission of Computer Codes)

37. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

38. On or about the dates set forth below, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and intentionally cause the transmission of a program, information, code and command, and as a result of such conduct, did intentionally cause

damage without authorization to a protected computer, and by such conduct caused loss to at least one person during a one-year period aggregating at least $5,000 in value, as set forth below:

COUNT	DATE	UNAUTHORIZED ACCESS
20	5/18/07	Packet sniffer installed on POS server at D&B Store #32 in Islandia, New York.
21	6/9/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York.
22	7/23/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York.
23	8/14/07	Packet sniffer reactivated on POS server at D&B Store #32 in Islandia, New York.

(Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(c)(4)(A), 2 and 3551 et seq.)

COUNTS TWENTY-FOUR THROUGH TWENTY-SEVEN
(Interception of Electronic Communications)

39. The allegations contained in paragraphs 1 through 14 are realleged and incorporated as if fully set forth in this paragraph.

40. On or about the dates set forth below, within the Eastern District of New York and elsewhere, the defendants MAKSYM YASTREMSKIY, also known as "Maksik," ALEKSANDR SUVOROV, also known as "JonnyHell," and ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and intentionally

intercept, endeavor to intercept, and procure another person to intercept, electronic communications, to wit: computer transmissions containing credit and debit card account numbers, as set forth below:

COUNT	DATES	INTERCEPTION
24	5/18/07 - 6/6/07	Packet sniffer capturing credit and debit card account numbers in transit from POS server at D&B Store #32 in Islandia, New York to data processor.
25	6/9/07 - 6/28/07	Packet sniffer capturing credit and debit card account numbers in transit from POS server at D&B Store #32 in Islandia, New York to data processor.
26	7/23/07 - 7/25/07	Packet sniffer capturing credit and debit card account numbers in transit from POS server at D&B Store #32 in Islandia, New York to data processor.
27	8/14/07 - 8/20/07	Packet sniffer capturing credit and debit card account numbers in transit from POS server at D&B Store #32 in Islandia, New York to data processor.

(Title 18, United States Code, Sections 2511(1)(a), 2511(4)(a), 2 and 3551 et seq.)

CRIMINAL FORFEITURE ALLEGATION FOR COUNTS ONE THROUGH FIVE

41. The United States hereby gives notice to the defendants charged in Counts One through Five that, upon their conviction of any such offense, the government will seek forfeiture in accordance with Title 18, United States Code, Section 981(a)(1)(C) and Title 28, United States Code, Section

2461(c), which require any person convicted of such offenses to forfeit any property constituting or derived from proceeds obtained directly or indirectly as a result of such offenses, for which the defendants are jointly and severally liable.

42. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States Code, Section 2461(c), to seek forfeiture of any other property of such defendant(s) up to the value of the forfeitable property described in this forfeiture allegation.

(Title 28, United States Code, Section 2461(c); Title 18, United States Code, Section 981(a)(1)(C); Title 21, United States Code, Section 853(p))

CRIMINAL FORFEITURE ALLEGATION FOR COUNTS
SIX THROUGH NINE AND THIRTEEN THROUGH TWENTY-THREE

43. The United States hereby gives notice to the defendants charged in Counts Six through Nine and Thirteen through Twenty-Three that, upon their conviction of any such offense, the government will seek forfeiture in accordance with Title 18, United States Code, Section 982(a)(2)(B), which requires any person convicted of such offenses to forfeit any property constituting or derived from proceeds obtained directly or indirectly as a result of such offenses, representing the proceeds obtained as a result of such offenses, for which the defendants are jointly and severally liable.

44. If any of the above-described forfeitable property, as a result of any act or omission of the defendants:

(a) cannot be located upon the exercise of due diligence;

(b) has been transferred or sold to, or deposited with, a third party;

(c) has been placed beyond the jurisdiction of the court;

(d) has been substantially diminished in value; or

(e) has been commingled with other property which cannot be divided without difficulty;

it is the intent of the United States, pursuant to Title 21, United States Code, Section 853(p), to seek forfeiture of any

other property of such defendant(s) up to the value of the forfeitable property described in this forfeiture allegation.

(Title 18, United States Code, Section 982(a)(2)(B); Title 21, United States Code, Section 853(p))

A TRUE BILL

FOREPERSON

BENTON J. CAMPBELL
UNITED STATES ATTORNEY
EASTERN DISTRICT OF NEW YORK

BY: _____
ACTING UNITED STATES ATTORNEY
PURSUANT TO 28 C.F.R. 0.138

FORM DBD-34
JUN. 85

No.

UNITED STATES DISTRICT COURT

EASTERN *District of* NEW YORK

CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

Maksym Yastremskiy, also known as "Maksik," Aleksandr Suvorov, also known as "JonnyHell," and Albert Gonzalez, also known as "Segvec,"

Defendants.

INDICTMENT

(T. 18, U.S.C., §§ 371, 981(a)(1)(C), 982(a)(2)(B), 1028A(a)(1), 1028A(b), 1028A(c)(5), 1029(a)(3), 1029(b)(2), 1029(c)(1)(A)(i), 1030(a)(2)(C), 1030(a)(4), 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(c)(2)(B)(i), 1030(c)(3)(A), 1030(c)(4)(A), 1343, 1349, 2511(1)(a), 2511(4)(a), 2 and 3551 et seq.; T. 21, U.S.C., § 853(p); T. 28, U.S.C., § 2461(c))

A true bill.

_____ *Foreman*

Filed in open court this _____ *day,*

of _____ *A.D. 20* _____

_____ *Clerk*

Bail, $ _____

William Campos, Assistant United States Attorney (631-715-7837)

Case 2:08-cr-00160-SJF-AKT Document 6 Filed 05/14/08 Page 24 of 24

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA	)	Criminal No. 08 CR 10223 PBS
	)	
v.	)	VIOLATIONS:
	)	18 U.S.C. § 371 (Conspiracy)
ALBERT GONZALEZ,	)	18 U.S.C. § 1030(a)(5)(A)(i) (Damage to Computer
a/k/a cumbajohny, a/k/a cj,	)	Systems)
a/k/a UIN 201679996, a/k/a	)	18 U.S.C. § 1343 (Wire Fraud)
UIN 476747, a/k/a soupnazi,	)	18 U.S.C. § 1029(a)(3) (Access Device Fraud)
a/k/a segvec, a/k/a k1ngchilli,	)	18 U.S.C. § 1028A (Aggravated Identity Theft)
a/k/a stanozololz,	)	18 U.S.C. §§ 1029(c)(1)(C), 982(a)(2)(B), 981(a)
	)	(1)(C), 28 U.S.C. §2461(c) (Criminal Forfeiture)
Defendant.	)	

INDICTMENT

COUNT ONE
(Conspiracy)
18 U.S.C. § 371

The Grand Jury charges that:

1. From approximately 2003 through 2008, in the Southern District of Florida, the District of Massachusetts, Eastern Europe and elsewhere, ALBERT GONZALEZ, Christopher Scott ("Scott"), Damon Patrick Toey ("Toey"), Maksym Yastremskiy ("Yastremskiy"), J.J., J.W., and others known and unknown to the Grand Jury, conspired to commit unlawful access to computer systems, in violation of 18 U.S.C. § 1030; wire fraud, in violation of 18 U.S.C. § 1343; access device (credit and debit card) fraud, in violation of 18 U.S.C. § 1029; aggravated identity theft, in violation of 18 U.S.C. §1028A; and money laundering, in violation of 18 U.S.C. § 1956.

Objects of the Conspiracy

2. The objects of the conspiracy were to:

a. Exploit vulnerabilities in wireless computer networks used at retail store locations;

b. Exploit vulnerabilities in software used to manage large business databases;

c. Gain unauthorized access to computer networks processing and storing debit and credit card transactions and other valuable data for major corporate retailers;

d. Download and steal from computer networks operated by major corporate retailers over 40 million pieces of card holders' track 2 data – the information found on the magnetic stripes of credit and debit cards, which is read by ATMs and credit card readers – as well as internal accounts and proprietary files;

e. Sell stolen track 2 data in Eastern Europe, the United States and elsewhere to others for their fraudulent use;

f. "Cash out" stolen track 2 data by encoding the data on the magnetic stripes of blank payment cards and using these cards to obtain tens of thousands of dollars at a time from banks' ATMs;

g. Conceal and launder the illegal proceeds through anonymous web currencies in the United States and Russia, and offshore bank accounts in Latvia; and

h. Repatriate portions of the illegal proceeds through web currency converters and ATM cards linked to Eastern European banks.

Manner and Means of the Conspiracy

3. In furtherance of the conspiracy, the conspirators – GONZALEZ, Scott, Toey, Yastremskiy, J.J., J.W., and others:

a. Went "wardriving" (driving around in a car with a laptop computer, looking for accessible wireless computer networks) in commercial areas of Miami, Florida, such as the area around U.S. 1;

b. Exploited wireless networks of retail store locations to gain unauthorized access to the networks that processed and stored credit and debit card transactions for major retailers including, but not limited to, BJ's Wholesale Club ("BJ's"), DSW, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, and TJX Companies ("TJX");

c. Located and stole sensitive files and data on these networks, including track 2 data and encrypted PIN blocks – the personal identifier numbers associated with debit cards;

d. Wrote, sought to obtain, and obtained from criminal associates in the United States and abroad, "sniffer" programs – programs which capture communications over computer networks – in order to monitor and steal (i) password and account information, which enabled the conspirators to access different computer servers containing payment card data within a corporate network, and (ii) track 2 data as it was moving across a network;

e. Downloaded from the corporate networks processing and/or storing payment card transactions the track 2 data for tens of millions of credit and debit cards and PIN blocks associated with millions of debit cards;

f. Obtained technical assistance from criminal associates in decrypting encrypted PIN numbers;

g. Obtained remote access to computer servers in the United States, Latvia and the Ukraine, in which the conspirators stored tens of millions of stolen credit and debit card numbers;

h. Encrypted those servers to conceal their purpose and prevent access by others;

i. Sold "dumps" – blocks of track 2 data – for fraudulent use, both in Eastern Europe and the United States;

j. "Cashed out" stolen track 2 data by encoding the data on the magnetic stripes of blank credit/debit cards and using these cards to obtain tens of thousands of dollars at a time from ATMs;

k. Moved money through anonymous web currency exchanges and bank accounts in Latvia to conceal the illegal proceeds;

l. Used foreign bank accounts to fund ATM cards, enabling conspirators to access the profits of their illegal activities from ATMs in the United States;

m. Using fictitious names, mailed express packages full of cash on a number of occasions to a drop box;

n. Used Internet-based attacks, often SQL injection attacks (which exploited security vulnerabilities in database-driven web sites), to find vulnerabilities and give the conspirators access to the track 2 data, internal accounts, and files of large businesses, including retailer Forever 21; and

o. Used sensitive law enforcement information, obtained by GONZALEZ during the course of his "cooperation" in a U.S. Secret Service undercover investigation, to warn off conspirators and ensure that they would not be identified and arrested in the course of that investigation.

Overt Acts of the Conspiracy

4. In furtherance of the conspiracy, GONZALEZ and his co-conspirators committed the following overt acts:

Compromising of Wireless Access Points

a. In or about 2003, GONZALEZ identified payment card data which was accessible at an unencrypted wireless access point utilized by a BJ's Wholesale Club store. GONZALEZ and Scott used this wireless access point to compromise track 2 data pertaining to BJ's customers. As used in this Indictment, "wireless access points" are devices that enable computers, including those in cash registers and inventory controllers, to connect with computer networks using radio waves.

b. In 2004, Scott, accompanied and assisted by J.J., gained unauthorized access to an OfficeMax wireless access point located near the intersection of 109th Street and U.S. 1, in Miami, Florida. The pair were able to locate

and download customers' track 2 debit card data, including encrypted PINs, on OfficeMax's payment card transaction processing network.

c. Contemporaneously, Scott and J.J. provided the data to GONZALEZ, who turned to another co-conspirator to decrypt the encrypted PINs.

d. On July 12 and 18, 2005, Scott compromised two wireless access points operated by TJX at Marshalls department stores in Miami, Florida. Scott used these access points repeatedly to transmit computer commands to TJX's computer servers processing and storing payment card transaction data in Framingham, Massachusetts.

e. On September 15-16, 2005 and November 18, 2005, the conspirators downloaded payment card data stored on TJX's servers in Framingham.

f. Beginning on May 14-15, 2006, Scott installed and configured a VPN connection from a TJX payment card transaction processing server to a server obtained by GONZALEZ. As used in this Indictment, a VPN, or "virtual private network," is a private or secure network connection within a public computer network, such as the Internet.

g. On May 15, 2006, GONZALEZ used ICQ (an instant messaging program) to ask Yastremskiy's assistance in obtaining an undetectable sniffer program. Beginning on May 15, 2006, and continuing for some days thereafter, including May 16, 18 and 20, Scott and his co-conspirators uploaded sniffer programs to a TJX payment card transaction processing server.

h. One of the sniffer programs uploaded by Scott and GONZALEZ was used to monitor and capture track 2 data as transactions were being processed by TJX's network. The track 2 data captured by the sniffer program was downloaded over the VPN on numerous dates, including October 27 and December 18, 2006.

Transition to Exploitation of Security Vulnerabilities in Database-Driven Web Sites

i. In approximately August of 2007, GONZALEZ invited Toey to move to Miami. In exchange for living rent-free in GONZALEZ's condominium and periodic cash payments, Toey collaborated with GONZALEZ on Internet-based attacks on corporate computer systems. These attacks, which included attacks on Forever 21, were aimed at obtaining financial data.

j. In the middle of October, 2007, GONZALEZ brought Scott to the condominium while Toey was there and, for the last time, they used a wireless access point of a nearby retailer as the vehicle for obtaining access to payment card transaction data.

Possession, Fraudulent Use and Sale of Credit and Debit Card Data

k. From 2004 through 2006, GONZALEZ sold track 2 data dumps through co-conspirator Toey by sending customers to Toey and by providing Toey with Internet locations where track 2 data dumps could be found.

l. During at least 2005 and the beginning of 2006, GONZALEZ provided dumps of track 2 data to J.W. J.W. encoded the information on the

magnetic stripes of blank payment cards, used the cards to obtain hundreds of thousands of dollars from ATMs, and split the money with GONZALEZ.

m. During a period which included February through May, 2006, GONZALEZ collaborated with international trafficker Yastremskiy to distribute the OfficeMax track 2 data.

n. On March 13, 2008, GONZALEZ connected via a VPN to a computer server in Latvia used by the conspirators to store malware (malicious software) and more than 16 million distinct credit and debit card numbers. From there, approximately 1 minute later, he logged on to a Ukranian server used by the conspirators to store files relating to TJX and more than 25 million distinct credit and debit card numbers.

Concealment of Proceeds

o. On dates including October 6, 2005 and October 19, 2005, J.W. sent bundles of cash for GONZALEZ by express mail to a drop box in Miami, Florida. The box had been leased by S.C., an unwitting individual, at the request of J.J.

p. Between approximately February 3, 2006, and May 24, 2006, Yastremskiy made approximately 20 electronic funds transfers, totaling more than $400,000, to GONZALEZ's numbered account at e-gold, Ltd., an online currency system. These transfers contained GONZALEZ's share of profits from the sale of track 2 data dumps.

Obstruction of Justice

q. In or about the fall of 2004, GONZALEZ warned Toey about an undercover criminal investigation in which GONZALEZ was providing assistance to the U.S. Secret Service. He did this to ensure that Toey would not be identified or arrested during the investigation.

Federal Offenses Involved in the Conspiracy

5. From approximately 2003 through 2008, in the Southern District of Florida, the District of Massachusetts, and elsewhere,

ALBERT GONZALEZ,

Scott, Toey, Yastremskiy, J.J., J.W., and others known and unknown to the Grand Jury, did willfully conspire to commit the following offenses against the United States:

a. Unlawful Access to Computers (18 U.S.C. § 1030(a)(2)(C)) – by means of interstate communications, intentionally accessing without authorization computers, which were used in interstate commerce, and thereby obtaining information from those computers, including credit and debit card information, for the purpose of commercial advantage and private financial gain;

b. Wire Fraud (18 U.S.C. § 1343) – having devised and executed a scheme to defraud, and to obtain money and property by means of false and fraudulent pretenses, representations, and promises, transmitting and causing to be transmitted, in interstate commerce, wire communications, including writings, signs and signals, for the purpose of executing the

scheme to defraud;

c. Access Device Fraud (18 U.S.C. § 1029(a)(3)) – knowingly and with intent to defraud, possessing at least fifteen unauthorized access devices – to wit: stolen credit and debit card numbers;

d. Aggravated Identity Theft (18 U.S.C. § 1028A) – knowingly transferring, possessing and using without lawful authority, means of identification of other persons – to wit: credit and debit card account numbers of individuals – during and in relation to the commission of wire fraud (in violation of 18 U.S.C. § 1343);

e. Money Laundering (18 U.S.C. §1956(a)(1)(B)(i) and (a)(2)(B)(i)) – knowing that the transactions, transmittals and transfers were designed in whole and in part to conceal and disguise the nature, location, source, ownership, and control of the proceeds of specified unlawful activity and that the property involved in the financial transactions represented the proceeds of some form of unlawful activity, (i) knowingly conducting and attempting to conduct financial transactions affecting interstate and foreign commerce, which involved the proceeds of said specified unlawful activity, and (ii) knowingly transmitting and transferring funds from a place inside the United States to and through a place outside the United States and to a place inside the United States from and through a place outside of the United States.

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

COUNTS TWO THROUGH SIX
(Damage to Computer Systems – 18 U.S.C. §1030(a)(5)(A)(i))

6. The Grand Jury realleges and incorporates by reference paragraphs 1 through 4 of this Indictment, and further charges that:

7. On or about the following dates, in the Southern District of Florida, the District of Massachusetts, and elsewhere,

ALBERT GONZALEZ

knowingly caused, and aided and abetted the cause of, the transmission of a program, information, code, and command, from a computer in Miami, Florida, to a computer utilized by TJX Companies in Framingham, Massachusetts, and as a result of such conduct, did intentionally cause damage without authorization to a computer used in interstate commerce and communication, and by such conduct caused loss to at least one person during a one-year period aggregating at least $5,000 in value, as set forth below:

Count	Date
Two	July 18, 2005
Three	May 14-15, 2006
Four	May 16, 2006
Five	May 18, 2006
Six	May 20, 2006

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), and 2.

COUNTS SEVEN THROUGH TEN
(Wire Fraud - 18 U.S.C. § 1343)

8. The Grand Jury realleges and incorporates by reference paragraphs 1 through 4 of this Indictment, and further charges that:

9. On or about the following dates, in the Southern District of Florida, the District of Massachusetts, and elsewhere,

ALBERT GONZALEZ,

having devised a scheme to defraud and to obtain money and property by means of false and fraudulent pretenses, representations and promises, transmitted and caused to be transmitted by wire in interstate commerce, for the purpose of executing the scheme to defraud, writings, signs and signals, to wit: interstate wire communications to computers in Framingham, Massachusetts used by TJX to process and store records of payment card transactions, as set forth below:

Count	Date
Seven	September 15-16, 2005
Eight	November 18, 2005
Nine	October 27, 2006
Ten	December 18, 2006

All in violation of Title 18, United States Code, Sections 1343 and 2.

COUNTS ELEVEN THROUGH FIFTEEN
(Access Device Fraud - 18 U.S.C. § 1029(a)(3))

10. The Grand Jury realleges and incorporates by reference paragraphs 1 through 4 of this Indictment, and further charges that:

11. On or about the following dates, in the Southern District of Florida, the District of Massachusetts, and elsewhere:

ALBERT GONZALEZ

knowingly, and with intent to defraud, possessed, and aided and abetted the possession of, at least 15 unauthorized access devices, to wit: stolen credit and debit card numbers, as set forth below:

Count	Date
Eleven	September 15-16, 2005
Twelve	November 18, 2005
Thirteen	October 3, 2006
Fourteen	October 27, 2006
Fifteen	December 18, 2006

All in violation of Title 18, United States Code, Sections 1029(a)(3) and 2.

COUNTS SIXTEEN THROUGH NINETEEN
(Aggravated Identity Theft - 18 U.S.C. § 1028A)

12. The Grand Jury realleges and incorporates by reference paragraphs 1 through 4 of this Indictment, and further charges that:

13. On or about the following dates, in the Southern District of Florida, the District of Massachusetts and elsewhere,

ALBERT GONZALEZ

knowingly transferred, possessed, and used, and aided and abetted the transfer, possession and use of, without lawful authority, means of identification of other persons – to wit: credit and debit card account numbers of individuals – during and in relation to the commission of wire fraud, a felony violation of 18 U.S.C. §1343, as set forth below:

Count	Date
Sixteen	September 15-16, 2005
Seventeen	November 18, 2005
Eighteen	October 27, 2006
Nineteen	December 18, 2006

All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.

FORFEITURE ALLEGATIONS
18 U.S.C. § 1029(c)(1)(C)
18 U.S.C. § 982(a)(2)(B)
18 U.S.C. § 981(a)(1)(C)
28 U.S.C. § 2461(c)

14. Upon conviction of one or more offenses in violation of 18 U.S.C. § 1029, charged in Counts Eleven through Fifteen of this Indictment, and/or § 1030, charged in Counts Two through Six herein,

ALBERT GONZALEZ,

defendant herein, shall forfeit to the United States any property constituting, or derived from, proceeds obtained directly or indirectly, as the result of one or more of the offenses, pursuant to 18 U.S.C. § 982(a)(2)(B). Such property includes, but is not limited to:

a. approximately $1,650,000.00 in United States currency;

b. the condominium located at 3855 SW 79th Avenue, Apt. 52, Miami, Florida, more particularly described in the Special Warranty Deed recorded on August 12, 2005 by the Miami-Dade County Clerk of Court at Book 23676, Page 1288;

c. one blue 2006 BMW 330I, bearing Vehicle Identification No. WBAVB33506KS37669;

d. approximately $6,700.00 in United States currency, seized from Albert Gonzalez on May 7, 2008;

e. approximately $15,823.00 in United States currency, seized from Albert Gonazlez on May 7, 2008;

f. one IBM Laptop Computer, Serial No. L3-AD488, seized from National Hotel, Room 1508, 1677 Collins Avenue, Miami, Florida on May 7, 2008;

g. one Toshiba Laptop Computer, Serial No. X5040-119H, seized from National Hotel, Room 1508, 1677 Collins Avenue, Miami, Florida on May 7, 2008;

h. a Glock 27 firearm, Serial No. GSZ729, along with ammunition, seized from National Hotel, Room 1508, 1677 Collins Avenue, Miami, Florida on May 7, 2008;

i. one Nokia cell phone, Serial No. 0516774LN01AF, seized from National Hotel, Room 1508, 1677 Collins Avenue, Miami, Florida on May 7, 2008;

j. one Everex Stepnote computer, Serial No. A07519663R, seized from 6400 SW 32nd Street, Miami, Florida on May 7, 2008;

k. one 350C Currency Counter, Serial No. J764265, seized from 6400 SW 32nd Street, Miami, Florida on May 7, 2008;

l. one Maxtor 300GB hard drive, Serial No. B60QLCYH, seized from 6400 SW 32nd Street, Miami, Florida on May 7, 2008;

m. one Sharp Zaurus PDA, Serial No. 63007505, seized from 6400 SW 32nd Street, Miami, Florida on May 7, 2008; and

n. approximately $178.87 in United States currency seized from the person and automobile of Albert Gonzalez on May 8, 2008;

(collectively, the "Assets").

15. Upon conviction of one or more offense in violation of 18 U.S.C. § 1029, charged in Counts Eleven Through Fifteen of this Indictment, § 1030, charged in Counts Two through Six herein, and/or §1343, charged in Counts Seven through Ten herein,

ALBERT GONZALEZ,

defendant herein, shall forfeit to the United States any property, real or personal, which constitutes or is derived from proceeds traceable to one or more of the offenses, pursuant to 18 U.S.C. § 981(a)(1)(C) and 20 U.S.C. § 2461(c). Such property includes, without limitation, the Assets.

16. Upon conviction or one of more offenses in violation of 18 U.S.C. § 1029, charged in Counts Eleven through Fifteen of this Indictment,

ALBERT GONZALEZ

defendant herein, shall forfeit to the United States any personal property used or intended to be used to commit the offense, pursuant to 18 U.S.C. § 1029(c)(1)(C). Such property includes, without limitation, the Assets listed in subparagraphs 13(c) through (n) above.

17. If any of the property described in paragraphs 14 through 16, as a result of any act or omission by the defendant –

a. cannot be located upon the exercise of due diligence,

b. has been transferred or sold to, or deposited with, a third party,

c. has been placed beyond the jurisdiction of the Court,

d. has been substantially diminished in value, or

e. has been commingled with other property which cannot be subdivided without difficulty,

it is the intention of the United States, pursuant to 18 U.S.C. § 1029(c)(2), 18 U.S.C. § 982(b)(1), and/or 28 U.S.C. § 2461(c), all of which incorporate 21 U.S.C. § 853(p), to seek forfeiture of any other property of the defendant up to the value of the property described above.

All pursuant to Title 18, United States Code, Sections 981, 982 and 1029, and Title 28, United States Code, Section 2461.

A TRUE BILL

Foreperson of the Grand Jury

Stephen P. Heymann
Assistant U.S. Attorney

DISTRICT OF MASSACHUSETTS August 5, 2008

Returned into the District Court by the Grand Jurors and filed.

Deputy Clerk
11:20 8/5 ms

SRK/EL/2009R00080

UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY

UNITED STATES OF AMERICA	:	Hon. JBS
	:	
v.	:	Criminal No. 09-626
	:	
	:	18 U.S.C. §§ 371 and 1349
ALBERT GONZALEZ,	:	
a/k/a "segvec,"	:	
a/k/a "soupnazi,"	:	
a/k/a "j4guar17,"	:	
HACKER 1, and	:	
HACKER 2	:	

INDICTMENT

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

COUNT 1
(Conspiracy)
18 U.S.C. § 371

1. At various times relevant to this Indictment:

The Defendants

a. Defendant Albert Gonzalez, a/k/a "segvec," a/k/a "soupnazi," a/k/a "j4guar17" ("GONZALEZ"), resided in or near Miami, Florida.

b. Defendant HACKER 1 resided in or near Russia.

c. Defendant HACKER 2 resided in or near Russia.

Coconspirator

d. P.T., a coconspirator who is not charged as a defendant herein, resided in or near Virginia Beach, Virginia and in or near Miami, Florida.

Methods of Hacking Utilized by Defendants

e. Structured Query Language ("SQL") was a computer programming language designed to retrieve and manage data on computer databases.

f. "SQL Injection Attacks" were methods of hacking into and gaining unauthorized access to computers connected to the Internet.

g. "SQL Injection Strings" were a series of instructions to computers used by hackers in furtherance of SQL Injection Attacks.

h. "Malware" was malicious computer software programmed to, among other things, identify, store, and export information on computers that were hacked, including information such as credit and debit card numbers and corresponding personal identification information of cardholders ("Card Data"), as well as to evade detection by anti-virus programs running on those computers.

The Corporate Victims of Computer Hacking

i. Heartland Payment Systems, Inc. ("Heartland"), which was located in or near Princeton, New Jersey and Plano, Texas, among other places, was one of the world's largest credit and debit card payment processing companies. Heartland processed millions of credit and debit transactions daily. Beginning on or about December 26, 2007, Heartland was the victim of a SQL

Injection Attack on its corporate computer network that resulted in malware being placed on its payment processing system and the theft of more than approximately 130 million credit and debit card numbers and corresponding Card Data.

j. 7-Eleven, Inc. ("7-Eleven") was the corporate parent of a convenience store chain that processed credit and debit card payments through its computer networks. Beginning in or about August 2007, 7-Eleven was the victim of a SQL Injection Attack that resulted in malware being placed on its network and the theft of an undetermined number of credit and debit card numbers and corresponding Card Data.

k. Hannaford Brothers Co. ("Hannaford") was a regional supermarket chain with stores located in Maine, New Hampshire, Vermont, Massachusetts, and New York that processed credit and debit card payments through its computer network. In or about early November 2007, a related company of Hannaford was the victim of a SQL Injection Attack that resulted in the later placement of malware on Hannaford's network and the theft of approximately 4.2 million credit and debit card numbers and corresponding Card Data.

l. Company A was a major national retailer that processed credit card payments through its computer network. Beginning on or about October 23, 2007, Company A was the victim of a SQL Injection Attack that resulted in the placement of

malware on its network.

m. Company B was a major national retailer that processed credit and debit card payments through its computer network. In or about January 2008, Company B was the victim of a SQL Injection Attack that resulted in the placement of malware on its network.

n. Heartland, 7-Eleven, Hannaford, Company A and Company B are collectively referred to herein as the "Corporate Victims."

THE CONSPIRACY

2. Between in or about October 2006 and in or about May 2008, in Mercer and Morris Counties, in the District of New Jersey, and elsewhere, defendants

ALBERT GONZALEZ,
a/k/a "segvec,"
a/k/a "soupnazi,"
a/k/a "j4guar17,"
HACKER 1, and
HACKER 2

did knowingly and intentionally conspire and agree with each other, P.T., and others to commit offenses against the United States, namely:

(a) by means of interstate communications, knowingly and intentionally accessing computers in interstate commerce without authorization, and thereby obtaining information from those computers, namely credit and debit card numbers and corresponding

Card Data, for the purpose of commercial advantage and private financial gain, contrary to Title 18, United States Code, Section 1030(a)(2);

(b) knowingly and with intent to defraud accessing computers in interstate commerce and exceeding authorized access to such computers, and by means of such conduct furthering the intended fraud and obtaining anything of value, namely credit and debit card numbers and corresponding Card Data, contrary to Title 18, United States Code, Section 1030(a)(4); and

(c) knowingly causing the transmission of programs, information, codes, and commands, and as a result of such conduct, intentionally causing damage without authorization to computers in interstate commerce, contrary to Title 18, United States Code, Sections 1030(a)(5)(A)(i) and (a)(5)(B)(i).

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy for GONZALEZ, HACKER 1, HACKER 2, P.T., and others to hack into the Corporate Victims' computer networks in order to steal credit and debit card numbers and corresponding Card Data from those networks, which credit and debit card numbers and other information was offered for sale in order to reap profits for the coconspirators.

MANNER AND MEANS OF THE CONSPIRACY

Scouting Potential Victims

4. It was part of the conspiracy that GONZALEZ and P.T. would identify potential corporate victims, by, among other methods, reviewing a list of Fortune 500 companies.

5. It was further part of the conspiracy that GONZALEZ and P.T. would travel to retail stores of potential corporate victims, both to identify the payment processing systems that the would-be victims used at their point of sale terminals (e.g., "checkout" computers) and to understand the potential vulnerabilities of those systems.

6. It was further part of the conspiracy that P.T. would also visit potential corporate victims' websites to identify the payment processing systems that the would-be corporate victims used and to understand the potential vulnerabilities of those systems.

Launching the Attacks - The Hacking Platforms

7. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would lease, control, and use Internet-connected computers in New Jersey ("the Net Access Server"), California ("the ESTHOST Server"), Illinois ("the Gigenet Server"), Latvia ("the Latvian Server"), the Netherlands ("the Leaseweb Server"), and Ukraine ("the Ukranian Server") (collectively, "the Hacking Platforms") to (1) store malware;

(2) stage attacks on the Corporate Victims' networks; and (3) receive credit and debit card numbers and corresponding Card Data from those networks.

8. It was further part of the conspiracy that GONZALEZ would provide HACKER 1, HACKER 2, and P.T. with SQL Injection Strings and malware that could be used to gain unauthorized access to the Corporate Victims' networks and to locate, store, and transmit credit and debit card numbers and corresponding Card Data stolen from those networks.

9. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would hack into the Corporate Victims' networks using various techniques, including, among others, SQL Injection Attacks, to steal, among other things, credit and debit card numbers and corresponding Card Data.

Executing the Attacks - The Malware

10. It was further part of the conspiracy that once they hacked into the computer networks, GONZALEZ, HACKER 1, and HACKER 2 would place unique malware on the Corporate Victims' networks that would enable them to access these networks at a later date ("Back Doors").

11. It was further part of the conspiracy that once they hacked into the Corporate Victims' networks, GONZALEZ, HACKER 1, and HACKER 2 would conduct network reconnaissance to find credit and debit card numbers and corresponding Card Data within the

Corporate Victims' networks.

12. It was further part of the conspiracy that once GONZALEZ, HACKER 1, and HACKER 2 hacked into the Corporate Victims' networks, they would install "sniffer" programs that would capture credit and debit card numbers, corresponding Card Data, and other information on a real-time basis as the information moved through the Corporate Victims' credit and debit card processing networks, and then periodically transmit that information to the coconspirators.

13. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would communicate via instant messaging services while the unauthorized access by them was taking place in order to advise each other as to how to navigate the Corporate Victims' networks and how to locate credit and debit card numbers and corresponding Card Data.

14. It was further part of the conspiracy that GONZALEZ, HACKER 1, and HACKER 2 would use unique malware to transmit the stolen credit and debit card information and Card Data to a Hacking Platform.

Concealing the Attacks

15. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would conceal their efforts to hack into the Corporate Victims' networks by, among other things, leasing the Hacking Platforms under false names, communicating

over the Internet using more than one messaging screen name, storing data related to their attacks on multiple Hacking Platforms, disabling programs that logged inbound and outbound traffic over the Hacking Platforms, and disguising, through the use of "proxies," the Internet Protocol addresses from which their attacks originated.

16. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would conceal their efforts to hack into the Corporate Victims' networks by, among other things, programming malware to be placed on the Corporate Victims' computer networks to evade detection by anti-virus software and then testing the malware against approximately 20 different anti-virus programs.

17. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. programmed the malware to be placed on the Corporate Victims' computer networks to erase computer files that would otherwise evidence its presence on the Corporate Victims' networks.

OVERT ACTS

18. In furtherance of the conspiracy, and to effect its unlawful object, the coconspirators committed and caused to be committed the following overt acts, among others, in the District of New Jersey and elsewhere:

a. On or about November 6, 2007, GONZALEZ transferred a computer file to the Ukranian Server named "sqlz.txt" that contained information stolen from Company A's computer network.

b. On or about November 6, 2007, GONZALEZ transferred a computer file to the Ukranian Server named "injector.exe" that matched malware placed on both Heartland and Company A's servers during the hacks of those companies.

c. On or about December 26, 2007, HACKER 1 and HACKER 2 accessed Heartland's computer network by means of a SQL Injection Attack from the Leaseweb Server and using the ESTHOST Server.

d. In or about January 2008, over an internet messaging service, GONZALEZ sent P.T. a SQL Injection String that was used to penetrate Company B's computer network (the "Company B SQL String"). The Company B SQL String was programmed to direct data to Hacking Platforms, including the ESTHOST Server and the Ukranian Server.

e. On or about March 13, 2008, at approximately 10:41 p.m., GONZALEZ connected to the Latvian Server.

f. On or about March 13, 2008, at approximately 10:42 p.m., GONZALEZ connected to the Ukranian Server.

g. On or about April 22, 2008, GONZALEZ modified a file on the Ukranian Server that contained computer log data stolen from Company B's computer network.

h. Between in or after March 2007 and in or about May 2008, GONZALEZ participated in a discussion over an internet messaging service in which one of the participants stated "planning my second phase against Hannaford."

i. Between in or after March 2007 and in or about May 2008, GONZALEZ participated in a discussion over an internet messaging service in which one of the participants stated "core still hasn't downloaded that [Company B] sh-t."

j. Between in or after December 2007 and in or about May 2008, P.T. participated in a discussion over an internet messaging service in which one of the participants stated "that's how [HACKER 2] hacked Hannaford."

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

COUNT 2
(Conspiracy to Commit Wire Fraud)
18 U.S.C. § 1349

1. The allegations contained in paragraphs 1 and 3 through 18 of Count 1 of the Indictment are realleged and incorporated as if set forth herein.

2. Between in or about October 2006 and in or about May 2008, in Morris and Mercer Counties, in the District of New Jersey, and elsewhere, defendants

ALBERT GONZALEZ,
a/k/a "segvec,"
a/k/a "soupnazi,"
a/k/a "j4guar17,"
HACKER 1, and
HACKER 2

did knowingly and intentionally conspire and agree to devise a scheme and artifice to defraud the Corporate Victims, their customers, and the financial institutions that issued credit and debit 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, to transmit and cause to be transmitted, by means of wire communication in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

OBJECT OF THE CONSPIRACY

3. It was the object of the conspiracy for GONZALEZ, HACKER 1, HACKER 2, P.T., and others to profit from the sale and fraudulent use of credit and debit card numbers and corresponding Card Data stolen from the Corporate Victims' computer networks.

MANNER AND MEANS OF THE CONSPIRACY

4. It was part of the conspiracy that once the coconspirators had stolen credit and debit card numbers and corresponding Card Data (the "Stolen Data") from the Corporate Victims' computer networks, GONZALES, HACKER 1, HACKER 2, and P.T. would cause the Stolen Data to be broken down into batches suitable for wholesale distribution over the Internet.

5. It was further part of the conspiracy that GONZALEZ, HACKER 1, HACKER 2, and P.T. would sell the Stolen Data and cause it to be available for resale.

6. It was further part of the conspiracy that those who purchased batches of the Stolen Data would further distribute the Stolen Data throughout the United States and elsewhere, where it would be used to make unauthorized purchases at retail locations, to make unauthorized withdrawals from banks and financial institutions, and to further identity theft schemes.

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

A TRUE BILL

FOREPERSON

Ralph J. Marra, Jr.

RALPH J. MARRA, JR.
Acting United States Attorney

CASE NUMBER: 09cr626-JBS

United States District Court
District of New Jersey

UNITED STATES OF AMERICA

v.

ALBERT GONZALEZ,
a/k/a "segvec,"
a/k/a "soupnazi,"
a/k/a "j4guar17,"
HACKER 1, and
HACKER 2

INDICTMENT

18 U.S.C. § 371
18 U.S.C. § 1349

RALPH J. MARRA, JR.
ACTING U.S. ATTORNEY
NEWARK, NEW JERSEY

SETH B. KOSTO/EREZ LIEBERMANN
ASSISTANT U.S. ATTORNEYS
(973) 645-2737/2874

USA-48AD 8 2009R00080
(Ed. 1/97)

Case 1:09-cr-00626-JBS Document 1 Filed 08/17/09 Page 15 of 15 PageID: 26