

UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

| | | |
|---------------------------------|---|--|
| UNITED STATES OF AMERICA |) | Criminal No. |
| |) | |
| 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 stanazololz, |) | 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 Ukrainian 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:

| <u>Count</u> | <u>Date</u> |
|--------------|-----------------|
| 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:

| <u>Count</u> | <u>Date</u> |
|--------------|-----------------------|
| 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:

| <u>Count</u> | <u>Date</u> |
|--------------|-----------------------|
| 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:

| <u>Count</u> | <u>Date</u> |
|--------------|-----------------------|
| 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 [REDACTED] 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 Gonzalez 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 [REDACTED] SW 32nd Street, Miami, Florida on May 7, 2008;
- k. one 350C Currency Counter, Serial No. J764265, seized from [REDACTED] SW 32nd Street, Miami, Florida on May 7, 2008;
- l. one Maxtor 300GB hard drive, Serial No. B60QLCYH, seized from [REDACTED] SW 32nd Street, Miami, Florida on May 7, 2008;
- m. one Sharp Zaurus PDA, Serial No. 63007505, seized from [REDACTED] 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.

