

**UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS**

_____)	
UNITED STATES OF AMERICA)	
)	
v.)	Criminal No. 09-10382-DPW
)	
ALBERT GONZALEZ,)	
)	
Defendant)	
_____)	

DECLARATION OF KEVIN G. WALSH

I, Kevin G. Walsh, hereby declare and state as follows:

1. I am an attorney admitted to practice in the states of New Jersey and New York, as well as the Federal District Courts for the District of New Jersey, the Southern District of New York, and the Eastern District of New York. I am a Director with the law firm of Gibbons P.C., counsel for Proposed Intervener Company A in this matter. I represent Company A, and specifically represented Company A in the District of New Jersey in this matter before it was transferred to the District of Massachusetts for plea and disposition pursuant to Rule 20, Fed.R.Crim.P.

2. The Indictment in the above-captioned matter generally charges a computer hacking conspiracy against Defendant Albert Gonzalez and two unnamed defendants. The Indictment alleges a "SQL Injection Attack" against Company A's computer systems. Attached as Exhibit A to this Declaration is a true and accurate copy of the Indictment in this matter. On pages three and four of that Indictment, Company A is identified as a victim of Defendant Gonzalez's alleged criminal conduct using only the pseudonym, "Company A." The government has not publicly disclosed Company A's identity throughout either the investigation or litigation stages of this case.

3. This case began for Company A on or about May 28, 2009, when Company A received a subpoena duces tecum from a Grand Jury sitting in the District of New Jersey (“the May 28th Subpoena”) which was investigating an October 2007 SQL injection attack by computer hackers. United States Secret Service agents alerted Company A in approximately May 2008 that it had been attacked in or about October 2007. Prior to receiving that alert, Company A was wholly unaware that it had been previously victimized by computer hackers.

4. On or about July 15, 2009, a Company A corporate representative and I met with representatives of the United States Attorney’s Office for the District of New Jersey (“the New Jersey USAO”) to explain the grave risk of harm to Company A, its customers, and its business partners that would arise if the Government’s investigation were to ripen into a criminal prosecution that necessitated unfettered Rule 16 discovery and inspection by one or more defendants with respect to evidence produced to the Grand Jury by Company A. The New Jersey USAO’s representatives provided assurances to Company A that the victim’s concerns regarding dignity, privacy, and anonymity would be considered at all stages of any prospective criminal prosecution, along with Company A’s unique concerns for its security, proprietary, and competitive interests.

5. On or about July 17, 2009, Company A complied with the May 28th Subpoena by providing to the United States Secret Service extensive electronic and paper information constituting proprietary, business-sensitive information that describes the security and design of Company A’s computer system data, images of such data, and other non-public commercial information (“the Company A Business Information”).

6. Throughout summer 2009, the New Jersey USAO assured me as counsel for Company A that the government would not publicly disclose Company A’s identity and would

otherwise respect the victim's concerns about keeping the Company A Business Information confidential, subject to the requirements of Fed. R. Crim. P. 16, the District of New Jersey's standing discovery order, and any further orders of the Court. The New Jersey USAO's representatives informed me that one of several reasons they agreed not to disclose Company A's identity publicly (whereas it had done so with respect to other victims of defendant Gonzalez's alleged criminal conduct) was that, although there had been a SQL injection attack, there was no evidence that Company A's customers' credit card data had been "exfiltrated" to computer servers controlled by defendant Gonzalez and his co-conspirators.

7. Attached to this Declaration as Exhibit B are true and accurate copies of correspondence exchanged between my law firm as counsel for Company A and the New Jersey USAO's representatives. These letters demonstrate that over many months Company A requested, among other things, that it not be identified publicly in this matter. See June 23, 2009 letter, at 2; July 17, 2009 letter, at 1-2. The Indictment and the subsequent press statement issued by the New Jersey USAO, which is attached hereto as Exhibit C, reflect that this request was honored. Indeed, the government has never publicly disclosed Company A's identity.

8. In addition to forbearing from disclosing Company A's identity publicly, the New Jersey USAO indicated its willingness to negotiate the terms of a stipulated protective order designed to protect Company A's interests during the litigation of this matter. To that end, on or about July 10, 2009, one of the Assistant U.S. Attorneys leading the New Jersey USAO's investigation provided me with sample protective orders that had been used to regulate defense counsel's access to discovery in the matters of United States v. Maxim Yastremskiy, Cr. No. 08-160 (E.D.N.Y.) and United States v. Albert Gonzalez, Cr. No. 08-160 (E.D.N.Y.) (the latter of which has resulted in a plea of guilty by Defendant Gonzalez, along with a plea of guilty to

federal criminal conduct arising from activities in the District of Massachusetts). Over many weeks, the New Jersey USAO and I agreed that a protective order in this matter should be entered by the Court in order to account for Company A's unique privacy needs and business concerns prior to the provision of Rule 16 discovery to the defendant and defense counsel. The New Jersey USAO recognized those needs and committed to working with Company A to reach agreement on the terms of a protective order.

9. I attach as examples of these discussions the materials attached hereto as Exhibit D, namely, true and accurate copies of letters dated August 19, 2009 and November 12, 2009, from me to the New Jersey USAO regarding the proposed protective order. In response, the New Jersey USAO wrote to me on November 12, 2009 and agreed that it would "not provide copies of discovery materials to defendant Gonzalez or his counsel until an appropriate protective order is in place," and agreed to "continue to act in accordance with the Victim Rights Act, Title 18, United States Code, Section 3771." A true and accurate copy of the government's November 12th letter is attached hereto as Exhibit E.

Pursuant to 28 U.S.C. §1746, I certify under penalty of perjury that the foregoing is true and correct. Executed this 24th day of December, 2009 in Newark, New Jersey.

s/ Kevin G. Walsh

Kevin G. Walsh

CERTIFICATE OF SERVICE

I hereby certify that this document was served via electronic mail this 24th day of December 2009:

Stephen P. Heymann, Esq.
United States Attorney's Office
1 Courthouse Way
Suite 9200
Boston, MA 02110
Stephen.heyman@usdoj.gov

Martin G. Weinberg
Martin G. Weinberg, PC
20 Park Plaza
Suite 1000
Boston, MA 02116
owlmcb@att.net

/s/ Michael D. Ricciuti
Michael D. Ricciuti

Exhibit A

SMK/ML/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 Ukrainian 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 Ukrainian 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 Ukrainian 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 Ukrainian Server.

g. On or about April 22, 2008, GONZALEZ modified a file on the Ukrainian 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-68AD § 2009R00080
(Ed. 1/97)

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

Exhibit B



KEVIN G. WALSH
Director

Gibbons P.C.
One Gateway Center
Newark, New Jersey 07102-5316
Direct: (973) 596-4789 Fax: (973) 639-6470
kwash@gibbonslaw.com

**CONFIDENTIAL COMMUNICATION
CONCERNING GRAND JURY INVESTIGATION**

June 23, 2009

BY ELECTRONIC MAIL

Assistant U.S. Attorney Erez Liebermann
Assistant U.S. Attorney Seth B. Kosto
Office of the United States Attorney
District of New Jersey
970 Broad Street
Newark, New Jersey 07102

Re: **Grand Jury Investigation**

Dear Gentlemen:

This firm represents ██████████ in connection with a subpoena dated May 28, 2009, that the government directed to the attention of ██████████ ("the Subpoena"). I write to confirm and amplify our telephone conversation from yesterday afternoon regarding this matter. As I explained during our telephone call, a corporate representative from ██████████ has formally requested to confer with you and your immediate supervisor, AUSA Judith H. Germano, in order to explain issues relating to, among other things, ██████████'s dignity and privacy as the alleged victim of a crime. See 18 U.S.C. §§ 3771(a)(5) & (a)(8).

██████████'s entire business consists of selling merchandise and services to customers through point of sale systems in its stores, as well as through the Internet and catalogs. These transactions are captured on the computer systems that are the subject of the subpoena. The subpoena requests ██████████ to produce records relating to work it performed internally with respect to the security of these systems. ██████████'s ability to maintain the security of its systems is crucial to the success of its business. Release of information about the design of ██████████'s computer systems to persons with criminal intent is likely to cause more damage to ██████████ and its customers and employees whose personal information is stored therein, than any criminal activity that may have taken place in the past. Therefore, if the company does produce confidential, proprietary, and sensitive information about its computer systems, it is concerned about how this information will be handled after the grand jury process is completed. Although Fed. R. Crim. P. 6(e) governs your treatment of company information during the grand jury investigation, we have no understanding of what is contemplated during the pre-trial or trial phases of the prospective criminal prosecutions.

GIBBONS P.C.

AUSA Erez Liebermann
AUSA Seth B. Kosto
June 23, 2009
Page 2

[REDACTED] is also concerned about how the government may or may not use its name in charging documents and press releases. You may recall your statement from June 9, 2009, indicating that the government has recently been naming corporate victims in cybercrime cases, which does not square with your position yesterday that naming [REDACTED] "is an open issue." The idea of naming [REDACTED] as a victim is also inconsistent with the government's recent decision to keep private the identity of victims in United States v. Nusier, a copy of which was posted to your office's public affairs web site on or about June 12, 2009. We need clarity on the government's position on this issue of signal importance to [REDACTED] in order that we can weigh our options if you intend to disregard the victim's wishes not to be identified in a charging document and corresponding press release.

Indeed, consumer confidence in the security of [REDACTED]'s computer systems is almost as important as the reality of that security. Therefore, any public document or release that leads customers to conclude erroneously that [REDACTED] customer information is not safe will seriously damage its business.

Although we appreciate that the intent of the subpoena was to investigate criminal conduct and not a malicious effort by the government to disregard victims' rights as described in Section 3771, [REDACTED] is concerned that the full panoply of privacy rights that are usually afforded to victims are not being respected with regards to [REDACTED]'s alleged involvement as a victim of the crime that you are investigating. In short, [REDACTED] wants to be treated with fairness and respect. As such, the company has requested that its corporate representative be offered an audience in which to explain the various harms that will befall [REDACTED] if its business good will is irreparably harmed by being named as a victim of "computer hacking."

To that end, I explained to you during our telephone call that the [REDACTED] representative has family and personal obligations to which she must attend during the week of June 29, 2009, not to mention the government holiday on July 3, 2009. The following week, [REDACTED] is overseas on a family vacation, and he has indicated quite understandably that he wants to be a part of any discussion concerning this matter. Accordingly, we would like to schedule a meeting during the week of July 13, 2009, to discuss these complicated and sensitive issues. Concomitantly, and as a matter of professional courtesy, I am requesting that you adjourn the return date of the Subpoena from June 25, 2009, until after we have had this opportunity to explain fully to you and Ms. Germano the risks that this subpoena creates for [REDACTED]. Please let me know if this is acceptable to the government. As always, I can be reached directly at 973-596-4769.

GIBBONS P.C.

AUSA Erez Liebermann
AUSA Seth B. Kosto
June 23, 2009
Page 3

Thank you for your continuing attention to this matter.

Very truly yours,



Kevin G. Walsh
Director

cc: [REDACTED] (by e-mail)
Robert M. Hanna, Esq. (by e-mail)
Judith H. Germano, AUSA (by e-mail)



ROBERT M. HANNA
Director

Gibbons P.C.
One Gateway Center
Newark, New Jersey 07102-3310
Direct: (973) 590-4501 Fax: (973) 639-0277
rhanna@gibbonslaw.com

**CONFIDENTIAL COMMUNICATION
CONCERNING GRAND JURY INVESTIGATION**

July 17, 2009

BY HAND DELIVERY

Assistant U.S. Attorney Erez Liebermann
Assistant U.S. Attorney Seth B. Kosto
Office of the United States Attorney
District of New Jersey
970 Broad Street
Newark, New Jersey 07102

Re: Grand Jury Investigation

Dear Counsel:

We write in connection with the grand jury subpoena dated May 28, 2009, that the government directed to the attention of [REDACTED] ("the Subpoena") at [REDACTED] ("the Company").

As we have discussed with you during the past six weeks, the Company asserts the attorney-client privilege and attorney work product protection as to all aspects of the Company's attorney-supervised investigation of the relevant incident described in the Subpoena, namely, the activities about which the USSS notified the Company on or about May 14, 2008. That investigation was conducted by Company personnel, IBM and MANDIANT under the supervision of Company attorneys. Documents relating to the company's retention of IBM and MANDIANT are enclosed as responsive, non-privileged documents.

We also want to thank you for meeting with [REDACTED] and us on July 15, 2009. The Company, which takes customer data security very seriously and prides itself on its exemplary corporate citizenship, has significant concerns as a victim of a crime under investigation by the grand jury. We trust that, as your office's investigation proceeds, you will be mindful of the Company's concerns and make every effort to ensure that the company is accorded its rights as a victim of crime. See 18 U.S.C. § 3771(c). We discussed during our July 15th meeting, for example, the company's very real concern that a public disclosure associating the company with data compromise could significantly damage the Company's well-earned, exemplary reputation with the public, as well as its relationships with existing and potential customers and third party credit

GIBBONS P.C.

**CONFIDENTIAL COMMUNICATION
CONCERNING GRAND JURY INVESTIGATION**

AUSA Erez Liebermann & AUSA Seth B. Kosto
July 17, 2009
Page 2

card companies. As your office's investigation develops the facts, we trust you will keep in mind various options available to you, including that you may be able to achieve your law enforcement goals without any reference to the Company in a charging document. Please continue to communicate with us concerning this possibility during the progress of your investigation, including the provision of as much advance notice as possible if your office ultimately decides to file any charging document referring directly or indirectly to the Company as the victim of a crime. As we have discussed, and absent exigent circumstances, in no event should such notice period be less than two weeks. Please know that the Company reserves all of its rights under 18 U.S.C. § 3771 and all other applicable laws that vindicate the rights of crime victims.

When we met with you on July 15, 2009, we also discussed that grave risks of harm to the Company and its customers and business partners would arise should your investigation ever ripen into an indictment necessitating Rule 16 discovery and inspection by one or more defendants of materials produced by the Company. We recognize that these concerns, as well as similar concerns arising from possible Rule 17 subpoenas and trial proofs, are somewhat premature at this time and may never ripen. Nevertheless, we appreciate your expressed willingness to work with us, should it become necessary, to develop appropriate protections that will safeguard the business, security and privacy interests of the Company and its customers and partners.

Regarding the Subpoena, we enclose responsive, non-privileged documents that have been stamped 000001 through 000101. In addition, and as we discussed by telephone this afternoon, non-privileged electronic data responsive to the subpoena is available for pick-up at the company's headquarters at [REDACTED]. This electronic data consists of forensic images of company servers and workstations, as well as firewall logs. You are authorized to have the United States Secret Service ("USSS") directly contact [REDACTED] Esq., the Company's Vice President, Associate General Counsel, to make arrangements for the government to obtain the electronic data today. [REDACTED] can be reached at ([REDACTED]) [REDACTED]-[REDACTED] or via e-mail at [REDACTED].

Pursuant to Schedule A, paragraph 4, of the Subpoena, the following information is responsive: [REDACTED], Delivery Manager, IBM Internet Services; [REDACTED], Delivery Manager, IBM Internet Services; [REDACTED], Manger Emergency Response Services, IBM Internet Services; [REDACTED], Engineer, IBM Internet Services; [REDACTED], Engineer, IBM Internet Services; [REDACTED], IBM Account Executive for [REDACTED]; [REDACTED], President, Mandiant; [REDACTED], Vice President Professional Services, Mandiant; [REDACTED], Principal Engineer, Mandiant; [REDACTED]

GIBBONS P.C.

**CONFIDENTIAL COMMUNICATION
CONCERNING GRAND JURY INVESTIGATION**

AUSA Erez Liebermann & AUSA Seth B. Kosto
July 17, 2009
Page 3

[REDACTED], Engineer, Mandiant; [REDACTED] Engineer, Mandiant; [REDACTED] Engineer,
Mandiant.

You should also know that, in or about June 2008, representatives from Visa contacted the Company based upon information that Visa said it had obtained from law enforcement. We have located documents regarding the Company's communications with Visa, but do not believe they are responsive to the Subpoena.

In furnishing this letter to the government, the Company intends to assert all lawful and legitimate privileges available to it. By producing non-privileged, responsive documents and information in response to the Subpoena, the Company does not intend to waive in whole or in part (inadvertently or otherwise) any lawful and legitimate privilege. The Company is continuing its search for non-privileged documents responsive to the Subpoena. We will keep you apprised of our progress.

We would welcome your telephone call or e-mail message if you need to speak with Kevin Walsh or me.

Very truly yours,



Robert M. Hanna
Director

Enclosures

cc: [REDACTED] (by e-mail)

Exhibit C



NEWS

United States Department of Justice
U.S. Attorney, District of New Jersey
970 Broad Street, Seventh Floor
Newark, New Jersey 07102



Ralph J. Marra, Jr., Acting U.S. Attorney

More Information? Call the Assistant U.S. Attorney or other contact listed below to see if more information is available.

News on the Internet: News Releases, related documents and advisories are posted short-term at our website, along with links to our archived releases at the Department of Justice in Washington, D.C. **Go to:** <http://www.usdoj.gov/usao/nj/press/>

Assistant U.S. Attorneys

SETH KOSTO

EREZ LIEBERMANN

gonz0817.rel

FOR IMMEDIATE RELEASE

Aug. 17, 2009

Three Men Indicted for Hacking into Five Corporate Entities, including Heartland, 7-Eleven, and Hannaford, With Over 130 Million Credit and Debit Card Numbers Stolen

(More)

Public Affairs Office
<http://www.njusao.org>
Michael Drewniak, PAO

973-645-2888

Breaking News (NJ) <http://www.usdoj.gov/usao/nj/press/index.html>

NEWARK, N.J. – An Indictment was returned today against three individuals who are charged with being responsible for five corporate data breaches, including the single largest reported data breach in U.S. history, announced Acting U.S. Attorney Ralph J. Marra, Jr., along with Assistant Attorney General of the Criminal Division Lanny A. Breuer and United States Secret Service Director Mark Sullivan.

The scheme is believed to constitute the largest hacking and identity theft case ever prosecuted by the U.S. Department of Justice.

The Indictment describes a scheme in which more than 130 million credit and debit card numbers together with account information were stolen from Heartland Payment Systems, Inc., based in Princeton, N.J., 7-Eleven, Inc., and Hannaford Brothers Co. In addition, the Indictment describes two unidentified corporate victims as being hacked by the coconspirators.

As alleged in the Indictment, between October 2006 and May 2008, Albert Gonzalez, 28, of Miami, Fla., acted with two unnamed coconspirators to identify large corporations, often by scanning the list of Fortune 500 companies and exploring corporate websites. Upon identifying a potential victim, Gonzalez and his coconspirators sought to identify vulnerabilities, both by physical observation and by online exploration. For example, according to the Indictment, Gonzalez and an individual identified in the Indictment as "P.T." would go to the retail locations of their potential victims in an attempt to identify the type of point-of-sale ("checkout") machines utilized by the victim companies. After reconnaissance of the computer systems was completed, information would be uploaded to servers which served as hacking platforms. These servers, located in New Jersey and around the world, were used by the coconspirators to store information critical to the hacking schemes and to subsequently launch the hacking attacks.

According to the Indictment, the hacking attacks launched against the corporate victims consisted of what is known as a SQL-injection attack, which is an attack that exploits security vulnerabilities in elements of a computer that receives user input. Gonzalez provided some of the malicious software (malware) to his coconspirators, and they added their own as they sought to identify the location of credit and debit card numbers and other valuable data on the corporate victims' computer systems.

The coconspirators often worked together on a real-time basis, contacting each other by instant messaging as they were improperly accessing the corporate victims' computer systems, according to the Indictment. Once the target information was discovered, it would be stolen from the corporate victims' servers and placed onto servers controlled by Gonzalez and the coconspirators. In addition to searching for credit and debit card data on the victims' computer systems, the Indictment alleges that Gonzalez and the coconspirators installed "sniffers" which conducted real-time interception of credit and debit card data being processed by the corporate victims and subsequently stolen from the corporate victims' computer servers.

The Indictment alleges that Gonzalez and the coconspirators employed numerous techniques to hide their hacking efforts and data breaches. For example, they allegedly accessed the corporate websites only through intermediary, or "proxy," computers, thereby disguising their own whereabouts. They also tested their malware by using approximately twenty of the leading anti-virus products to determine if any of those products would detect their malware as potentially unwanted. Furthermore, they programmed their malware to actively delete traces of the malware's presence from the corporate victims' networks.

Upon stealing the credit and debit card data, Gonzalez and the coconspirators would seek to sell the data to others who would use it to make fraudulent purchases, make unauthorized withdrawals from banks and further identity theft schemes.

"This investigation marks the continued success of law enforcement in tracking down cutting edge hacking schemes committed by hackers working together across the globe," said Marra. Marra added that the investigation was greatly facilitated by those companies that took a proactive approach in working with law enforcement to identify and stop hackers. "When companies make the decision to work with law enforcement and disclose a data breach at the earliest possible opportunity, it provides the best chance at apprehending a hacker and demonstrates that those corporate victims will actively defend their systems."

A federal grand jury sitting in Newark, N.J., charged Gonzalez and two individuals identified only as "Hacker 1," and "Hacker 2," both in or near Russia, in the two-count Indictment. The first count charges conspiracy to (1) gain unauthorized access to computers, (2) commit fraud in connection with computers, and (3) damage computers. The second count charges conspiracy to commit wire fraud. Each defendant faces a maximum penalty of 5 years in prison on Count One and an additional 30 years on Count Two, for a total of 35 years. In addition, each of the individuals is subject to a maximum fine of \$250,000 per Count One, and \$1 million per Count Two, or twice the gain resulting from the offense, whichever is greater.

Gonzalez was previously indicted in the Eastern District of New York on May 12, 2008, and the District of Massachusetts on August 5, 2008, for his involvement in different conspiracies relating to data breaches of multiple companies. He was also previously arrested in New Jersey in 2003 for his role in ATM and debit card fraud. Gonzalez is currently detained in the Metropolitan Detention Center in Brooklyn, New York.

Marra credited the Special Agents of the United States Secret Service, under the direction of Special Agent in Charge Cynthia Wofford, for their work in the investigation.

An Indictment is merely an accusation, and all defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt.

The case is being prosecuted by Assistant U.S. Attorneys Seth Kosto and Erez Liebermann of the U.S. Attorney's Office Computer Hacking and Intellectual Property Section, part of the Commercial Crimes Unit in Newark, New Jersey, and Senior Counsel Kimberly Kiefer

Peretti of the Criminal Division's Computer Crime & Intellectual Property Section.

-end-

Exhibit D



KEVIN G. WALSH
Director

Gibbons P.C.
One Gateway Center
Newark, New Jersey 07102-5310
Direct: (973) 596-4769 Fax: (973) 639-6470
kw Walsh@gibbonslaw.com

**CONFIDENTIAL COMMUNICATION
CONCERNING VICTIM ISSUES**

August 19, 2009

BY ELECTRONIC AND REGULAR MAIL

Assistant U.S. Attorney Erez Liebermann
Assistant U.S. Attorney Seth B. Kosto
Office of the United States Attorney
District of New Jersey
970 Broad Street
Newark, New Jersey 07102

Re: United States v. Albert Gonzalez, et al., Crim. No. 09-626 (JBS)

Dear Gentlemen:

As you know, this firm represents "Company A" as described in the above-referenced indictment returned by the grand jury on Monday. For many weeks now, Robert M. Hanna and I have been discussing with your office the ways in which Company A's rights as a victim can be protected throughout the life of your prosecution, from grand jury proceedings through sentencing. My client was disappointed that it was included in the indictment even as a pseudonym with a corresponding description. Nonetheless, in light of the Indictment and accompanying press releases, and especially given all of the media attention they have attracted, we would like to confirm and particularize the continuing efforts to protect Company A's business, security, and privacy interests that Mr. Hanna and I discussed with Deputy U.S. Attorney Marc P. Ferzan on Monday afternoon. Indeed, we previously raised this issue in our letter to you dated July 17, 2009, and we followed up with each of you since Monday on this topic.

We certainly believe that a Protective Order Governing Rule 16 Discovery must continue the anonymity protections that Company A currently enjoys, as well as protect and safeguard the business, security, and privacy interests of Company A and its customers and partners. To that end, we received from you several samples of protective orders on July 10, 2009, and in an effort to assist you, we will provide you shortly for discussion a draft protective order that reflects Company A's unique concerns. In addition to reaching ultimate agreement with the government regarding the terms of a protective order, we expect Company A's anonymity and business sensitive concerns to be respected throughout all stages of the prosecution, including but not limited to:

GIBBONS P.C.

CONFIDENTIAL COMMUNICATION
CONCERNING VICTIM ISSUES

AUSA Erez Liebermann
AUSA Seth B. Kosto
August 19, 2009
Page 2

- Pretrial, non-public Rule 16 disclosures to and inspection by defendants, defense counsel, and any experts (any such correspondence must be marked as non-public and confidential, pursuant to the forthcoming protective order);
- Rule 17 subpoenas (if custodians such as, for example, Mandiant receive subpoenas from defense counsel, the government must support the same levels of protection afforded to Company A as will exist in the forthcoming protective order);
- Plea proceedings, such that any plea agreement, plea memorandum to a U.S. District Judge, plea colloquy with a U.S. District Judge, and press release must respect the privacy rights and sensitive business concerns of Company A;
- Trial, such that all evidentiary issues must account for Company A's privacy and business concerns, and it may be necessary to create pseudonyms for use of certain evidence in court (the true identity of which pseudonyms might be known to defense counsel and the government, but will not be disseminated to the general public at trial); and
- Sentencing, such that all sentencing documents, including the government's press release must continue to respect the privacy rights and sensitive business concerns of Company A.

We expect to work closely with you to navigate these complex issues and to ensure that your prosecution is successful. We certainly hope your work results in guilty pleas, thereby obviating a public trial.

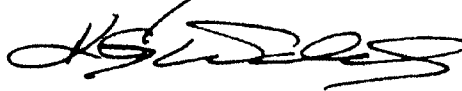
As we have advised you previously, consumer confidence in the security of Company A's computer systems is almost as important as the reality of that security. Therefore, any public document or release that leads customers to conclude erroneously that Company A's customer information is not safe will seriously damage its business. We will appreciate your continuing regard for Company A's privacy and business concerns, as well as for your attention to these important victim issues. Please know that Company A continues to reserve all of its rights under 18 U.S.C. § 3771 and all other applicable laws that vindicate the rights of crime victims.

GI^B BC NS PC

A^A US^A E^b z Lie^e
A^A A^r K^rrmann
US^S Se^h B. osto
A^u s 19, 2009
Page 3

CONFIDENTIAL COMMUNICATION
CONCERNING VICTIM ISSUES

Very truly yours,



Kevin G. Walsh
Director



KEVIN G. WALSH
Director

Gibbons P.C.
One Gateway Center
Newark, New Jersey 07102-5310
Direct: (973) 596-4769 Fax: (973) 639-6470
kwalsh@gibbonslaw.com

**CONFIDENTIAL COMMUNICATION FROM
VICTIM TO THE UNITED STATES ATTORNEY'S OFFICE**

November 12, 2009

BY ELECTRONIC MAIL

Assistant U.S. Attorney Erez Liebermann
Office of the United States Attorney
District of New Jersey
970 Broad Street
Newark, New Jersey 07102

Re: **United States v. Albert Gonzalez, Cr. No. 09-626 (JBS)**

Dear Erez:

I write to thank you for submitting to Judge Simandle the 30-day continuance order that governs the motion filing deadline for any protective order in the above-referenced matter. The judge's deputy clerk informs me that the order will be entered on the docket later today or tomorrow. I also want to confirm my understanding gained from our prior telephone conversations, namely, that in the absence of a signed protective order your Office will not be making available for inspection by defense counsel or Defendant Albert Gonzalez Rule 16 discovery (paper, electronic, or otherwise) that relates to Company A. If my understanding is mistaken, please notify me immediately.

Also, on behalf of Company A, I would still like to understand exactly how the CCAP works, so that the victim can gain a greater knowledge of the security of the system that is intended to facilitate defense counsel's review of Company A's electronic discovery materials. I will appreciate if you can furnish me with any explanatory materials in this regard. I reiterate again that the "who" and "how" of access to electronic and paper discovery that relates to Company A is an exceedingly important issue for this victim. I look forward to hearing from you about this issue.

Finally, if there are any public events scheduled in this case, please notify me (as you have been doing thus far) so that I can keep Company A apprised of developments in this matter. Thank you for your continuing attention to these victim issues.

Very truly yours,

Kevin G. Walsh
Director

Exhibit E



U.S. Department of Justice

*United States Attorney
District of New Jersey*

*Erez Liebermann
Assistant U.S. Attorney*

*970 Broad Street, Suite 700
Newark, New Jersey 07102*

*Telephone No. (973) 645-2874
Facsimile No. (973) 645-3497*

November 12, 2009

Kevin G. Walsh
Gibbons P.C.
One Gateway Center
Newark, New Jersey 07102

Re: United States v. Albert Gonzalez, 09-626

Dear Kevin:

We are writing in response to, and to clarify your letter dated November 12, 2009. We will not provide copies of discovery materials to defendant Gonzalez or his counsel until an appropriate protective order is in place. With regard to the CCAP, it is a secure computer mechanism for electronic discovery whereby access is restricted to authorized individuals. As you are aware, the Court in the District of Massachusetts approved the CCAP as a properly secure facility in a related litigation.

Please be advised that we have acted and will continue to act in accordance with the Victim Rights Act, Title 18, United States Code, Section 3771. If you have any further questions regarding the rights or concerns of your client-victim, please contact our Victim-Witness Coordinator, Shirley Estreicher, at 973-645-2893.

Very truly yours,

PAUL J. FISHMAN
United States Attorney

/s Erez Liebermann

By: EREZ LIEBERMANN
Assistant U.S. Attorney