WPC

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - - X

UNITED STATES OF AMERICA

    - against -

ALBERT GONZALEZ,
    also known as
    "Segvec,"

           Defendant.

- - - - - - - - - - - - - - - - X

O R D E R

08-M-444

       Upon the application of BENTON J. CAMPBELL, United

States Attorney for the Eastern District of New York, by

Assistant United States Attorney WILLIAM P. CAMPOS, it is hereby

       ORDERED that the Affidavit In Support of Arrest Warrant

in the above-captioned case be unsealed.

Dated: Central Islip, New York
         May 12, 2008

                                 _____
                                 UNITED STATES MAGISTRATE JUDGE
                                 EASTERN DISTRICT OF NEW YORK

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

- - - - - - - - - - - - - - - - - X 08 0444M   Filed Under Seal

UNITED STATES OF AMERICA

    - against -

ALBERT GONZALEZ,
    also known as "Segvec,"

             Defendant.

- - - - - - - - - - - - - - - - X

AFFIDAVIT IN SUPPORT
OF ARREST WARRANT

(18 U.S.C. § 1349)

EASTERN DISTRICT OF NEW YORK, ss:

    MATTHEW LYNCH being duly sworn, deposes and says that he is a Special Agent with the United States Secret Service ("USSS"), duly appointed according to law and acting as such:

    There is probable cause to believe that 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 defendant ALBERT GONZALEZ, also known as "Segvec," together with others, did knowingly and intentionally conspire to devise a scheme and artifice to defraud the national restaurant chain Dave & Buster's, Inc. ("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, Section 1349)

The basis for my information and the grounds for my belief are as follows:[1]/

1.   I have been a Special Agent with the USSS for approximately six (6) years. I have been assigned to the United States Secret Service Melville Resident Office for approximately four (4) years. My information in this case comes from conversations with other law enforcement officers, reports of other law enforcement officers, my review of various documents and records related to this investigation, and from my training and experience.

2.   Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part.

Dave & Buster's Intrusions

3.   The evidence obtained in the investigation revealed that, from approximately April through September of 2007, GONZALEZ, together with Aleksandr Suvorov and Maksym

---

[1]Because the purpose of this affidavit is to set forth only those facts necessary to establish probable cause, I have not set forth all of the facts and circumstances of which I am aware.

Yastremskiy, who are currently under a sealed indictment in the
Eastern District of New York for their conduct in the Dave &
Buster's intrusions, devised and executed a scheme to remotely
access, without authorization, the computer systems of D&B in
order to obtain credit and debit card account data that they
could sell to others who, in turn, would either use the data to
make fraudulent purchases or re-sell it to others to make such
purchases.

4.   Dave & Buster's, Inc. (D&B), is an American
restaurant chain with 49 locations in the United States.   In
September 2007, D&B contacted the USSS about unauthorized
computer intrusions that had occurred in their computer systems.
D&B had discovered that one or more persons had accessed, without
authorization, point-of-sale (POS) computer servers at some of
D&B's restaurants.   The POS computer servers were used to
transmit credit and debit card account data for D&B customers
through the D&B corporate network to a third party data processor
for authorization and verification.

5.   According to the forensic examination report of
the intrusion provided by D&B and confirmed by the USSS, the
first unauthorized access to a D&B POS computer server occurred
in April 2007, when someone used an Internet connection to
remotely access a POS server at a D&B restaurant in Arundel,
Maryland.   That person unsuccessfully tried to install computer
software, known as a packet sniffer, on the D&B computer.   A

packet sniffer refers to computer software that can intercept and record computer transmissions traveling from one networked computer to another networked computer. The packet sniffer that the intruder attempted to install here was a piece of malicious software designed to collect credit and debit card account numbers and expiration dates when such information was transmitted from the POS computer server at the Arundel, Maryland restaurant location through D&B's corporate computer systems in Dallas, Texas to the computer systems of a third party data processor. The packet sniffer malfunctioned, however, and no credit or debit card account information was captured.

6.   According to the D&B forensic report and confirmed by the USSS, on May 18, 2007, the intruders accessed D&B's corporate computer network in Dallas, Texas without authorization and, from there, successfully installed the packet sniffer on POS servers at 11 D&B restaurants, including one in Islandia, New York, in the Eastern District of New York.

7.   Specifically, on the Islandia POS server, the packet sniffer functioned correctly and collected credit and debit card account data for D&B customers who used their credit and debit cards to purchase food and other services at the restaurant. Once the packet sniffer collected this credit and debit card data, the packet sniffer stored the data in a computer log file that could later be retrieved and used for fraudulent purposes, such as creating counterfeit credit cards or making fraudulent credit card purchases. Additionally, the sniffer was

periodically reactivated because a defect in the packet sniffer's software program caused the packet sniffer to automatically deactivate whenever the compromised D&B POS servers rebooted in the normal course of the operation of the servers.

8. With respect to the Islandia D&B restaurant, the forensic examination report confirmed that the packet sniffer was actively collecting customers' credit and debit card account information during four time periods between May and September 2007: (1) May 18 through June 6, 2007; (2) June 6 through June 9, 2007; (3) July 23 through July 25, 2007; and (4) August 14 through August 20, 2007.

9. According to the D&B forensic report and confirmed by the USSS, on September 22, 2007, another attempt to access the Islandia POS server without authorization was made, but D&B had become aware of the previous intrusions by that time and had blocked the intruder from collecting any further credit and debit card data.

10. Investigation has revealed that approximately 5,100 MasterCard and Visa cards as well as 32 American Express cards were used in the D&B restaurant in Islandia during the time periods when the packet sniffer was actively collecting credit and debit card data. Further, 675 of these cards were subsequently used to make unauthorized purchases at various retail locations and from various online merchants worldwide, causing losses of at least $600,000 to the financial institutions that issued the credit and debit cards. This investigation has

confirmed that these credit and debit card account numbers were stolen when they were used at the D&B restaurant in Islandia, New York, and not another merchant or retailer.

Evidence Linking ICQ UIN 201679996 to the D&B Intrusion

11. GONZALEZ was eventually determined to be the provider of the packet sniffer used in the computer intrusions described above based on his association with a Ukrainian citizen, by the name of Maksym Ystremskiy, who was one of the biggest resellers of stolen credit card data targeted by the USSS.

12. In July 2007, Yastremskiy was arrested in Turkey by the Turkish National Police. This arrest was based, in part, on charges of trafficking in stolen credit card numbers, brought in the Southern District of California in connection with a USSS investigation in that district.

13. Around the time of Yastremskiy's arrest, the Turkish National Police seized Yastremskiy's laptop computer and cellular phone. The Turkish National Police, then, provided an image of the computer, along with Yastremskiy's computer password, to the USSS. Through the forensic examination, the USSS recovered information from Yastremskiy's laptop that related to the intrusions into the D&B computers. Specifically, the USSS found many stored ICQ instant messages sent over the Internet (referred to as "chat logs") on the laptop, millions of stolen credit card numbers, and a folder that contained a packet sniffer used in the D&B intrusions.

14. ICQ is an instant messaging service, similar to AOL's instant messaging service, which identifies its users by numbers, called "UIN." ICQ conversations, or chats, can be logged (recorded) by their participants.

15. The stored chat logs on Yastremskiy's laptop were essentially transcripts of instant messages between Yastremskiy and various associates. From these chat logs, the USSS was able to determine that Yastremskiy communicated with an individual using the UIN 201679996. The ICQ chat logs also reflect that the person using ICQ UIN 201679996 changed the ICQ UIN through which he was communicating with Maksik following news that one of the retailers that he (201679996) had compromised was uncovered and was being investigated. At that time, he stated that he would begin communicating with Maksik through ICQ UIN 476747. For simplicity and clarity, the ICQ UIN 201679996 is used throughout this Affidavit rather than switching between the two ICQ UINs.

16. The logs obtained from Maksik indicate that ICQ UIN 201679996 took credit for supplying the packet sniffer to Maksik to pass on to a third party, later determined to be Aleksandr Suvorov, for use in the D&B intrusions. For example, Maksik and ICQ UIN 201679996 exchanged the following messages before and after the successful installation of the packet sniffer on D&B computers on May 18, 2007:

- <u>May 15, 2007</u> (ICQ UIN 201679996 to Maksik): "btw, this plalce [sic] your guy hacked from db.rar is a very nice place, they have many locations, its called Dave & Buster's"

- May 15, 2007 (Maksik to ICQ UIN 201679996): "yeah db is dave and busters:-)"

- May 16, 2007 (Maksik to ICQ UIN 201679996): "Hi! i know how danb is working, just need sniffer listening to port 10700 in/out:-) could you,please recompile it:-) Thanks"

- May 16, 2007 (ICQ UIN 201679996 to Maksik): "i can compile it right now"

- May 18, 2007 (ICQ UIN 201679996 to Maksik): "did your guy use or say anything about my sniffer for dandb?"

- May 18, 2007 (Maksik to ICQ UIN 201679996): "my guy told me to tell you big thanks and etc :-)"

- May 24, 2007 (Maksik to ICQ UIN 201679996): "hackers waiting news from you about sniffer"

- May 24, 2007 (ICQ UIN 201679996 to Maksik): "i sent them sniffer for dandb"

- May 30, 2007 (ICQ UIN 201679996 to Maksik): "did your guy give any info on how things are going on d and b? im curious if my sniffer work or not"

- May 30, 2007 (Maksik to ICQ UIN 201679996): "about sniffer he told me. what exactly you are interested in ? he says it seems its working, he got 5gb log file"

The USSS confirmed that the packet sniffer referred to in these logs was installed on D&B computer systems on May 18, 2007 and captured Track 2 cardholder information until it was detected in September 2007.

17. ICQ UIN 201679996 also said that he had had the

packet sniffer customized for use in a prior intrusion of a major

retailer (hereinafter "Retailer One") in 2005, currently under

investigation by the USSS, and later described modifying the

sniffer program for Maksik's associate (Aleksandr Suvorov) to use

in the D&B intrusion. An analyst at the Computer Emergency

Response Team Coordinating Center (CERT-CC) has analyzed the

sniffers found on Retailer One's and Dave & Buster's systems. He

has confirmed that they appear to be two different versions of

the same program and that in his experience, this underlying

program is unique. The core sniffer program, according to the

CERT analyst, is efficient, well designed, and uses some

algorithms and data structures that reflect college-level

knowledge of computer programming skills, whether acquired

through self-study or, as he believed more likely, through formal

training.

Evidence Linking ICQ UIN 201679996 to GONZALEZ

18. Evidence described below strongly links the user

of ICQ UIN 201679996 to GONZALEZ.

19. As stated above, in the Maksik logs, ICQ UIN

201679996 took credit for having had a "sniffer" program

customized for use on Retailer One's financial-processing

servers. Additional forensic evidence indicates that the

Retailer One intruder transferred 44GB of payment card

information stolen from Retailer One to IP address 205.209.184.50

on November 18-19, 2005. According to logs of ICQ conversations obtained by Secret Service in a separate investigation, this IP address was assigned on these dates to ICQ UIN 201679996.

20. Confidential sources indicated that GONZALEZ uses the Internet nicknames "soupnazi" and "segvec." Both of these nicknames have been linked to the ICQ UIN 201679996, and in turn, to GONZALEZ. ICQ UIN 201679996 was originally registered with the e-mail address of soupnazi@efnet.ru. The forensic analysis of a computer seized from GONZALEZ following his arrest in 2003[2] indicates that he has used this e-mail address. Confidential Source 1 ("CS-1") has independently stated that Gonzalez used the screenname "soupnazi."

21. In a March 9, 2006 chat logged on Maksik's hard drive, ICQ UIN 201679996 expressed concern that a friend who was cashing cards for him had been arrested the day before. CS-1, who reported that he had been cashing cards for GONZALEZ, was arrested on March 8, 2006, the day before.

22. CS-1 stated, during a law-enforcement interview, that he had forwarded a picture of himself to GONZALEZ, who was going to get him a Netherlands passport. In the days immediately

---

[2] GONZALEZ was arrested in July, 2003, for access device fraud. Agents seized numerous computers from Gonzalez at the time of his arrest in 2003. On one of these computers were logs of Internet relay chat conversations in which he had participated three years earlier in 2000. (Internet relay chat is the electronic equivalent of a conference call.) During the chat, Gonzalez, using the screen name "soupnazi."

prior to CS-1's arrest, Maksik's ICQ chat logs contain negotiations between ICQ UIN 201679996 and Maksik about Maksik's obtaining for ICQ UIN 201679996 a passport from either the Netherlands or Russia for an initially unidentified individual. On March 9, 2006, ICQ UIN 201679996 identified the person for whom he had planned to obtain the Netherlands passport as being his friend who had just been arrested; as stated above, CS-1 was arrested that day.

23. During the course of their business dealings, Maksik's ICQ logs also reflect ICQ UIN 201679996 directing Maksik to wire ICQ UIN 201679996's share of the proceeds of fraudulently obtained card information to a bank account in Latvia. GONZALEZ similarly directed CS-1 to wire GONZALEZ' share of the proceeds of carding to bank accounts in Latvia on at least two occasions.

24. Following the announcement of the discovery of the Retailer One breach, the registration of ICQ UIN 201679996 was changed from soupnazi@efnet.ru (known to be used by GONZALEZ) to segvec@fromru.com. Records pertaining to E-gold, Ltd., a company issuing an internet currency called "e-gold," contain a transaction from an e-gold account also registered to the e-mail address segvec@fromru.com to SIA Ekosistems in Latvia. CS-1 was similarly directed by GONZALES to wire carding proceeds to the same entity, SIA Ekosistems, in Latvia.

25. GONZALEZ has also been linked to the nickname

"segvec" by Confidential Source 2 ("CS-2"), who stated, during a law-enforcement interview, that GONZALEZ has admitted to him that he (GONZALEZ) uses the Internet nicknames "soupnazi" and "segvec", among others. CS-2 also stated during the interview that he and GONZALEZ have been associated with several data breaches of large businesses.

26. Maksik's chat logs also link ICQ UIN 201679996 to the Internet nickname "segvec". Maksik used the nickname "segvec" on several occasions when referring directly or indirectly to the user of ICQ UIN 201679996. On October 20, 2006, Maksik stated that one of his friends was told he could obtain "pins" (i.e., personal identification numbers that cardholders use to prevent unauthorized transactions, and which criminals need to obtain direct cash withdrawals with stolen credit or debit card information) from "segvec." In response, the user of ICQ UIN 201679996 states "funny cuz I dont have shit". Additionally, on December 12, 2006, Maksik and the user of ICQ UIN 201679996 were discussing a published article on recent seizures of e-gold accounts, including Segvec's account, by the U.S. government. ICQ UIN 201679996 states that "they mention specific shit in the article [...] about my operations and yours."

WHEREFORE, your deponent respectfully requests that the Court issue a warrant for the arrest of defendant ALBERT GONZALEZ so that he may be dealt with according to law. Because this investigation is ongoing, I respectfully request that this affidavit be ordered filed under seal.

_____ 5/8/08

MATTHEW LYNCH
Special Agent
United States Secret Service

Sworn to before me this
8th day of May, 2008

_____
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

The affidavit shall be filed under seal and remain under seal until further order of the Court.

SO ORDERED:

_____
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

United States District Court

EASTERN   DISTRICT OF   NEW YORK

UNITED STATES OF AMERICA

V.

ALBERT GONZALEZ,
    also known as "segvec"

To: Special Agent Matthew Lynch, United States Secret Service
and any Authorized United States Officer

WARRANT FOR ARREST
CASE NUMBER:

08 0444M

YOU ARE HEREBY COMMANDED to arrest _____ **ALBERT GONZALEZ** _____
                                                         Name

and bring him forthwith to the nearest magistrate to answer a(n)

☐ Indictment   ☐ Information   ☒ Complaint   ☐ Order of court   ☐ Violation Notice   ☐ Probation Violation Petition

charging him with (brief description of offense)

conspiracy to commit wire fraud

in violation of Title **18** United States Code, Section(s) **1349** _____

Hon. Michael L. Orenstein	**UNITED STATES MAGISTRATE JUDGE**
Name of Issuing Officer	Title of Issuing Officer

Michael L. Orenstein (signature)
Signature of Issuing officer

May 8, 2008   Central Islip, New York
Date and Location

Bail fixed at $ _____   by _____
                                                              Name of Judicial Officer

---

RETURN

This warrant was received and executed with the arrest of the above-named defendant at _____

DATE RECEIVED	NAME AND TITLE OF ARRESTING OFFICER	SIGNATURE OF ARRESTING OFFICER
DATE OF ARREST		