

RPD:KKP:ECW  
F. #2007R01826

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

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF NEW YORK

★ MAY 14 2008 ★

----- X

LONG ISLAND OFFICE

UNITED STATES OF AMERICA

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

- against -

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

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

----- X

THE GRAND JURY CHARGES:

**INTRODUCTION**

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

The Victim Entity

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

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

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

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

parties that accepted credit and debit cards as payments.

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

#### THE SCHEME TO DEFRAUD

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

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

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

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

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

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

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

#### Intrusions at D&B Store #32

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

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

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

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

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

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

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

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

COUNT ONE

(Conspiracy to Commit Wire Fraud)

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

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

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

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

COUNTS TWO THROUGH FIVE  
(Wire Fraud)

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

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



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

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

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

COUNT SIX

(Conspiracy to Possess Unauthorized Access Devices)

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

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

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

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

OVERT ACTS

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

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

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

sniffer.

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

COUNTS SEVEN THROUGH NINE  
(Possession of Unauthorized Access Devices)

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

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

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

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

COUNT TEN

(Aggravated Identity Theft)

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

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

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

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

COUNT ELEVEN  
(Aggravated Identity Theft)

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

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

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

COUNT TWELVE  
(Aggravated Identity Theft)

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

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

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

COUNT THIRTEEN

(Conspiracy to Commit Computer Fraud)

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

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

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

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

OVERT ACTS

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

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

sniffer.

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

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

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

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

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



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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

CRIMINAL FORFEITURE ALLEGATION FOR COUNTS ONE THROUGH FIVE

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

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

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

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

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

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

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

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

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

- (a) cannot be located upon the exercise of due diligence;
- (b) has been transferred or sold to, or deposited with, a third party;
- (c) has been placed beyond the jurisdiction of the court;
- (d) has been substantially diminished in value; or
- (e) has been commingled with other property which cannot be divided without difficulty;

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

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


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

A TRUE BILL

FOREPERSON 

---

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

BY:   
ACTING UNITED STATES ATTORNEY  
PURSUANT TO 28 C.F.R. 0.136

No.

**UNITED STATES DISTRICT COURT**

EASTERN District of NEW YORK

CRIMINAL DIVISION

THE UNITED STATES OF AMERICA

vs.

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

Defendants.

**INDICTMENT**

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

*A true bill.*

Foreman

Filed in open court this \_\_\_\_\_ day,

of \_\_\_\_\_ A.D. 20 \_\_\_\_\_

Clerk

Bail, \$ \_\_\_\_\_

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