Presented to the Court by the foreman of the Grand Jury in open Court, in the presence of the Grand Jury and FILED in the U.S. DISTRICT COURT at Seattle, Washington.

MARCH 16 2011

WILLIAM M. McCOOL, Clerk

By _____ Deputy

Judge Richard A. Jones

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak. Defendant.	NO. CR11-070RAJ **SUPERSEDING INDICTMENT** **(SEALED)**

The Grand Jury charges that:

COUNTS 1 - 5

(Bank Fraud)

A. The Offense

1. Beginning at a time unknown, but no later than October 2, 2009, and continuing through on or about February 22, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus,

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

aka Zagreb, aka shmak (hereinafter Roman Seleznev), and others unknown to the Grand Jury, knowingly and willfully devised and executed, and aided and abetted a scheme and artifice to defraud various financial institutions, including, but not limited, to Boeing Employees' Credit Union ("BECU"), Chase Bank, Capital One, Citibank, and Keybank ("the banks"), financial institutions as defined by Title 18, United States Code, Section 20, and to obtain moneys, funds, and credits under the custody and control of the banks by means of material false and fraudulent pretenses, representations and promises, as further described below.

2. The object of the scheme and artifice to defraud was to "hack" into the computers of retail businesses within the Western District of Washington, and elsewhere; to install malicious computer code onto those hacked computers that would effectively steal the credit card numbers of the victim businesses' customers; to market and sell the stolen credit card numbers, on criminally inspired websites, for the purpose and with the intent that the stolen credit card numbers would then in turn be used for fraudulent transactions across the United States, and in foreign countries; and, by way of the scheme, to obtain illicit proceeds, funded by and derived primarily from the banks (located in the Western District of Washington, and elsewhere), that had originally issued the stolen credit card numbers. By way of this series of criminal actions, the defendants intended to and did generate and receive millions of dollars in illicit profits, that they then converted to their own personal benefit and use.

B. Manner and Means of the Scheme and Artifice to Defraud

3. ROMAN SELEZNEV has used "nics" or online nicknames in his dealings and his communications with others regarding and promoting the theft and sale of stolen credit card numbers that include: "TRACK2," "nCuX," "Bulba," "bandysli64," "smaus," "Zagreb," and "shmak."

4. It was part of the scheme and artifice to defraud that ROMAN SELEZNEV, and others unknown to the Grand Jury, created a criminally inspired, Internet-based

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

infrastructure to facilitate the theft, and then the sale, over the Internet, of credit card account numbers that had been issued by banks, including BECU.

5. It was further part of the scheme and artifice to defraud that, as part of that criminal Internet-based infrastructure, ROMAN SELEZNEV, and others unknown to the Grand Jury, rented, configured, and controlled server computers in countries outside of the United States, including the Ukraine and Russia, that contained malware, or malicious computer code, which servers would provide downloads of that malware, onto other computers, when the requesting computers were commanded to made such a request.

The server that hosted the malware was "named" "shmak.fvds.ru," aka "smaus.fvds.ru" aka "188.120.225.66" and all of the malware was located, on the server, at shmak.fvds.ru/<malwarenamehere>. The server stored pieces of malware that been denominated with names that included "shmak,""shmak2," "kameo," "hameo" "zameo" "dtc," "dtc2," "dtc4," "dtca," "rsca," "remcomsvc," and others. All of the malware was located at the root of the server.

6. It was further part of the scheme and artifice to defraud that, as part of that criminal Internet-based infrastructure, ROMAN SELEZNEV, and others unknown to the Grand Jury, rented and configured server computers in countries outside of the United States for the purpose of hosting carding forum websites, or websites used to sell stolen credit card numbers, including carding forums named, "bulba.cc," "secure.bulba.cc," "Track2.name" and "secure.Track2.name."

7. It was further part of the scheme and artifice to defraud that, as part of that criminal Internet-based infrastructure, ROMAN SELEZNEV, and others unknown to the Grand Jury, rented and configured server computers, including servers in McLean, Virginia, to receive and compile stolen credit card track data.

8. It was further part of the scheme and artifice to defraud that ROMAN SELEZNEV, and others unknown to the Grand Jury, developed and used automated techniques, such as port scanning, to identify computers and computer systems that were connected to the Internet, that were dedicated to or involved with credit card processing

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

by retail businesses, and that would be vulnerable to criminal hacks for the purpose of stealing credit card numbers.

9. It was further part of the scheme and artifice to defraud that ROMAN SELEZNEV, and others unknown to the Grand Jury, used those automated techniques to identify credit card processing computers at the Broadway Grill restaurant, and at other businesses in the Western District of Washington as well as throughout the United States, as target computers for their criminal scheme.

10. It was further part of the scheme and artifice to defraud that once ROMAN SELEZNEV, and others unknown to the Grand Jury, identified credit card processing computers that were vulnerable to criminal hacks, they issued commands to the target computers to connect, over the Internet, to the servers that they had previously rented and configured and that they controlled, in the Ukraine and Russia, and to download malware from those servers, so that it would be installed on the victim target computers.

Specifically, once ROMAN SELEZNEV, and others unknown to the Grand Jury had remote control of a victim computer, they would launch a web browser on the victim computer. They would then type the address for the server hosting the malware ("shmak.fvds.ru,") followed by the name of the piece of malware they wished to have downloaded (for example, "shmak.fvds.ru/kameo.exe"). The piece of malware specified could vary, as between the many different pieces of malware that were being hosted on the Ukraine/Russian server. Once this web address was typed into the address bar of the victim computer, the victim computer would download this piece of malware from the Ukraine/Russian server.

Once the malware was installed on the victim computer, ROMAN SELEZNEV, and others unknown to the Grand Jury, could disconnect from the victim computer. The malware that had been downloaded was preconfigured to upload credit card data that subsequently passed through the victim computer, to the server that had been designated by ROMAN SELEZNEV, and others unknown to the Grand Jury, for that purpose.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

In some cases ROMAN SELEZNEV, and others unknown to the Grand Jury, also installed a piece of software that would enable them to easily remotely reconnect to the victim servers again, at a later date.

11. It was further part of the scheme and artifice to defraud that the malware that ROMAN SELEZNEV, and others unknown to the Grand Jury caused to be installed on the targeted victim computers included software that monitored network activity within the business' internal computer network. The businesses that were targeted typically had several computers running, including a few "point of sale" terminals, and/or other computers that employees used to process orders, and to swipe customer credit cards when purchases were made. These computers were in turn connected to a computer, commonly referred to as the "the back of the house computer," or the "manager's computer," that would receive all of the credit card track data that had been gathered from the point of sale terminals; encrypt that data; and transmit it to the merchant card processor for approval.

The malware that ROMAN SELEZNEV, and others unknown to the Grand Jury caused to be downloaded to the victim business' computers monitored the traffic within the business' computer network and intercepted the communications between the point of sale terminals and the back of the house computer. The malware would extract and copy the data that included credit card track data and, every five minutes, compile the stolen credit card track data and transmit and upload it to a server identified by a specified IP address. That server had been previously rented and configured and was controlled by ROMAN SELEZNEV, and others unknown to the Grand Jury, for that purpose, and could be located in a variety of geographic locations, including in Russia, the Ukraine, or, for a time, in McLean, Virginia.

12. It was further part of the scheme and artifice to defraud that one of the business computer networks that was found vulnerable, and was hacked by ROMAN SELEZNEV and others unknown to the Grand Jury, was that of the Broadway Grill restaurant, in Seattle, WA. In the case of the Broadway Grill, in particular, every credit

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

card number that had been swiped at the restaurant between December 1, 2009, and October 22, 2010, (over 32,000 unique credit card numbers) had been saved to a text file that was stored on the business' back of the house computer. ROMAN SELEZNEV, and others unknown to the Grand Jury, commanded the computer they hacked at the Broadway Grill restaurant to steal, transmit, and upload that complete text file, containing all of those unique credit card numbers, to computer servers specified by ROMAN SELEZNEV, and others unknown to the Grand Jury, that had previously been rented and configured and that were under their control, for that purpose.

ROMAN SELEZNEV, and others unknown to the Grand Jury, also caused and commanded the DTC2.exe malware to be installed on the manager's credit card processing computer at the Broadway Grill, in the manner described above, which malware then continued to steal any additional credit card track data, including credit card numbers, run after October 22, 2010. That data, as well, was transmitted from the infected Broadway Grill computer over the Internet, to computer servers specified, configured, and controlled by ROMAN SELEZNEV, and others unknown to the Grand Jury, for that purpose. The theft of credit card track data from Broadway Grill continued thereafter until the intrusion and theft were discovered on October 27, 2010.

13. It was further part of the scheme and artifice to defraud that, using the same techniques described above that were used to hack into, install malware, and steal credit card track data from the Broadway Grill restaurant in Seattle, WA, ROMAN SELEZNEV, and others unknown to the Grand Jury, hacked into, installed malware, and stole credit card tract data from a number of other small retail businesses in the Western District of Washington including, but not limited to: Grand Central Baking Company restaurant, in Seattle, WA; four Mad Pizza restaurants (three Seattle, WA, locations and a location in Tukwila, WA); Village Pizza, in Anacortes, WA, and Casa Mia Italian restaurant, in Yelm, WA.

14. It was further part of the scheme and artifice to defraud that, using the same techniques described above that were used to hack into, install malware, and steal credit

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

card track data from the Broadway Grill restaurant and other businesses in the Western District of Washington, ROMAN SELEZNEV, and others unknown to the Grand Jury likewise hacked into, installed malware, and stole credit card tract data from hundreds of retail businesses in other locations throughout the United States, including, but not limited to: Schlotzsky's Deli, in Coeur d'Alene, Idaho; Active Networks, in Frostburg, Maryland; Days Jewelry, in Waterville, Maine; Latitude Bar and Grill, in New York, New York; Grand Canyon Theatre, in Tusayan, Arizona; the Phoenix Zoo, in Phoenix, Arizona; Mary's Pizza Shack, in Sonoma, California; and City News Stand (a convenience store), at multiple store locations in Evanston, and Chicago, Illinois.

15. It was further part of the scheme and artifice to defraud that after credit card track data was transmitted from hacked businesses, and then compiled on the servers that ROMAN SELEZNEV, and others unknown to the Grand Jury had previously rented, configured, and controlled for that purpose, ROMAN SELEZNEV, and others unknown to the Grand Jury, harvested the data, and extracted and segregated from it credit card account numbers, Bank Identification Numbers ("BIN numbers,") and any other data possible, including names of the account holders or PIN numbers, that would enhance the value of the data for sale to those who wished to use it for criminal fraudulent purposes.

16. It was further part of the scheme and artifice to defraud that after ROMAN SELEZNEV, and others unknown to the Grand Jury, had stolen, harvested, and segregated the data that was valuable for sale to their would-be criminal customers, they then posted and marketed that data for sale on carding forum websites, including those named, "bulba.cc" and "Track2.name," which websites they had established on computer servers that they had rented, configured, and which they controlled, for this purpose. The stolen credit card numbers that they marketed and sold on these carding forum websites included credit card numbers that had been issued by BECU, and by other banks in the Western District of Washington and throughout the United States.

17. It was further part of the scheme and artifice to defraud that when ROMAN SELEZNEV, and others unknown to the Grand Jury advertised and sold stolen credit card

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

numbers, BIN numbers, and related stolen data for sale on their carding forum websites, they priced that data at varying levels, depending on its relative worth for use in fraudulent transactions. For example, credit card numbers with a "95%" guarantee for validity were priced between $20 and $30 per credit card track. This comprised the majority of the cards listed for sale. There were also credit card numbers listed at lower, "sale" prices. These were listed with a guarantee of validity of around "65%," and were listed for sale at around $7 per track.

18. It was further part of the scheme and artifice to defraud that ROMAN SELEZNEV, and others unknown to the Grand Jury would seek to attract and entice customers to their carding forum websites by advertising "fresh dumps" of stolen data, which included, for example, an advertisement on November 24, 2010, as follows:

> UPDATE OF 38,000 USA (TRACK1+2) AND 5.000 USD
> TRACK2 ONLYTOTALLY MADE!!!
> 90% VALID! BIG BASE, NEW60 - TRACK1+TRACK2,
> NEW61 - TRACK2 ONLY

And through an advertisement on December 23, 2010, as follows:

> UPDATE 17,000 FRESH DUMPS TOTALY MADE! VALID
> VERY HIGH 95%!!
> 75% TRACK1 + TRACK2 AND OTHER TRACK2 ONLY!!!
> Base - NEW65
> Warning - today checker not work at all. Sorry for that .
> Merry XMAS!:). THAT IS THE LAST UPDATE IN THIS YEAR. Hurry up to fund account

19. It was further part of the scheme and artifice to defraud that ROMAN SELEZNEV, and others unknown to the Grand Jury, sought to enhance the value and to spur sales of the stolen credit card data they marketed, for fraudulent use, by offering a "checker" service through the carding forum websites, which, for a fee, would enable customers to obtain instant validation information for the stolen credit card numbers, and

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

through which they also offered to "replace" numbers that were found to be invalid through the checking service with an equal number of other stolen credit card numbers.

20. It was further part of the scheme and artifice to defraud that ROMAN SELEZNEV, and others unknown to the Grand Jury, who controlled and operated the bulba.cc and Track2.name carding forum websites, would only accept payment for the stolen data that they sold through a limited number of payment services, including webmoney services such as "Liberty Reserve," because those services hinder efforts to trace the proceeds of the transactions and effectively conceal the identity of both the payers and the recipients of the proceeds of the same.

21. It was further part of the scheme and artifice to defraud that, in order to expand and maximize their customer base for stolen credit card numbers, ROMAN SELEZNEV, and others unknown to the Grand Jury, advertised the carding forums that they owned and controlled on other well known carding forum websites, such as "crdsu.su" and "carder.biz."

22. It was further part of the scheme and artifice to defraud that, in order to quash competition from other criminal carders, ROMAN SELEZNEV, and others unknown to the Grand Jury, assumed total control and a monopoly over stolen credit card sales made on the previously established and preeminent carder forum website named "crdsu.su," in or around May of 2010.

23. It was further part of the scheme and artifice to defraud that ROMAN SELEZNEV, and others unknown to the Grand Jury, stole over 200,000 credit card numbers, and sold over 140,000 stolen credit card numbers through their carding forum websites, bulba.cc and Track2.name, during the period from November 15, 2010, to February 22, 2011.

24. It was further part of the scheme and artifice to defraud that ROMAN SELEZNEV, and others unknown to the Grand Jury, generated illicit profits totaling at least $2,000,000.00 from the sale of stolen credit card information on the bulba.cc and track2.name websites during the period from November 15, 2010, to February 22, 2011.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

25. It was further part of the scheme and artifice to defraud that the stolen credit card numbers sold by ROMAN SELEZNEV, and others unknown to the Grand Jury, have been used to commit fraudulent transactions throughout the United States, including specifically in the States of Texas and New York, and throughout the world.

26. It was further part of the scheme and artifice to defraud that credit card numbers, in particular, that were stolen from the Broadway Grill by ROMAN SELEZNEV, and others unknown to the Grand Jury, which credit card numbers had been issued by BECU, were used in fraudulent transactions after their sale on the bulba.cc and track2.name websites for fraudulent transactions that have caused losses to BECU of at least $79,317.00; and that credit card numbers stolen from Broadway Grill that were issued by other banks, and sold on the bulba.cc and Track2.name websites, have caused losses to the other banks that issued those cards in the amount of at least $1,763,140.56.

C. Execution of the Scheme and Artifice to Defraud

27. On or about the below-listed dates, within the Western District of Washington and elsewhere, for the purpose of executing and attempting to execute this scheme and artifice to defraud, ROMAN SELEZNEV, and others unknown to the Grand Jury, did knowingly and willfully steal the credit card account numbers specified below, that had been issued by BECU, which account numbers subsequently were used in fraudulent transactions, causing a loss to BECU in the amounts specified below:

Count	**Date CC # Stolen**	**CC Acct. Number** Issued by BECU	BECU Fraud Loss on Acct. No. Due to Fraudulent Transactions
1	10/22/2010	**********5719	$1199.59
2	10/22/2010	**********6316	$650.14
3	10/22/2010	**********7089	$636.86
4	10/22/2010	**********0016	$317.98
5	10/22/2010	**********0717	$394.60

All in violation of Title 18, United States Code, Sections 1344 and 2.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

COUNT 6

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On our about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on a credit card processing computer belonging to and located at the Broadway Grill restaurant, in Seattle, WA, and by such conduct caused loss to one or more persons during a one year period aggregating at least $5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i), and 2.

COUNT 7

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On our about October 2, 2009, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on a credit card processing computer belonging to and located at the Grand

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Central Baking Company restaurant, in Seattle, WA, and by such conduct caused loss to one or more persons during a one year period aggregating at least $5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i), and 2.

COUNT 8

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On our about August 28, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on a credit card processing computer belonging to and located at the Mad Pizza restaurant, in Tukwila, WA, and by such conduct caused loss to one or more persons during a one year period aggregating at least $5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i), and 2.

COUNT 9

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On our about November 2, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb,

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on a credit card processing computer belonging to and located at the Mad Pizza restaurant, 1263 Thomas Street, Seattle, WA, and by such conduct caused loss to one or more persons during a one year period aggregating at least $5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i), and 2.

COUNT 10

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On our about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on a credit card processing computer belonging to and located at the Mad Pizza restaurant, 1321 Madison St., Seattle, WA, and by such conduct caused loss to one or more persons during a one year period aggregating at least $5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i), and 2.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

COUNT 11

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On our about August 26, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on a credit card processing computer belonging to and located at the Mad Pizza restaurant, 4021 E. Madison St., Seattle, WA, and by such conduct caused loss to one or more persons during a one year period aggregating at least $5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i), and 2.

COUNT 12

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On our about September 13, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on a credit card processing computer belonging to and located at

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

the Village Pizza restaurant, in Anacortes, WA, and by such conduct caused loss to one or more persons during a one year period aggregating at least $5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i), and 2.

COUNT 13

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On our about August 9, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly caused the transmission of a program, information, code, and command, and as a result of that conduct, intentionally caused and attempted to cause damage, without authorization, to a protected computer, to wit, by causing the installation of malware on a credit card processing computer belonging to and located at the Casa Mia Italian Pizzeria restaurant, in Yelm, WA, and by such conduct caused loss to one or more persons during a one year period aggregating at least $5,000 in value.

All in violation of Title 18, United States Code, Sections 1030(a)(5)(A), and 1030(c)(4)(B)(i), and 2.

COUNT 14

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about October 22, 2010, and continuing until on or about October 27, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, they intentionally accessed a credit card processing computer belonging to and located at the Broadway Grill restaurant, in Seattle, WA, and obtained therefrom credit card track data that included credit card account numbers issued by Boeing Employees Credit Union or other financial institutions as defined by Title 18, United States Code, Section 20; and that they committed such offense in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States, specifically, bank fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii), and 2.

COUNT 15

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about October 2, 2009, and continuing until on or about December 1, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, they intentionally accessed a credit card processing computer belonging to and located at the Grand Central Baking Company restaurant, in Seattle, WA, and obtained therefrom credit card track data that included credit card account numbers issued by Boeing Employees Credit Union or other financial institutions as defined by Title 18, United States Code, Section 20; and that they committed such offense in furtherance of a criminal and tortious act in violation

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

of the Constitution and laws of the United States, specifically, bank fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii) and 2.

COUNT 16

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about August 28, 2010, and continuing until on or about February 1, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, they intentionally accessed a credit card processing computer belonging to and located at the Mad Pizza restaurant, in Tukwila, WA, and obtained therefrom credit card track data that included credit card account numbers issued by Boeing Employees Credit Union or other financial institutions as defined by Title 18, United States Code, Section 20; and that they committed such offense in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States, specifically, bank fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii) and 2.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

COUNT 17

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about November 2, 2010, and continuing until on or about February 1, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, they intentionally accessed a credit card processing computer belonging to and located at the Mad Pizza restaurant, 1263 Thomas St., Seattle, WA, and obtained therefrom credit card track data that included credit card account numbers issued by Boeing Employees Credit Union or other financial institutions as defined by Title 18, United States Code, Section 20; and that they committed such offense in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States, specifically, bank fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii) and 2.

COUNT 18

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about October 22, 2010, and continuing until on or about February 15, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus,

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, they intentionally accessed a credit card processing computer belonging to and located at the Mad Pizza restaurant, 1321 Madison St., Seattle, WA, and obtained therefrom credit card track data that included credit card account numbers issued by Boeing Employees Credit Union or other financial institutions as defined by Title 18, United States Code, Section 20; and that they committed such offense in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States, specifically, bank fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii) and 2.

COUNT 19

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about August 26, 2010, and continuing until on or about February 15, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, they intentionally accessed a credit card processing computer belonging to and located at the Mad Pizza restaurant, 4021 E. Madison St., Seattle, WA, and obtained therefrom credit card track data that included credit card account numbers issued by Boeing Employees Credit Union or other financial institutions as defined by Title 18, United States Code, Section 20; and that they committed such offense in furtherance of a criminal and tortious act in violation

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

of the Constitution and laws of the United States, specifically, bank fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii) and 2.

COUNT 20

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about September 25, 2010, and continuing until on or about February 8, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, they intentionally accessed a credit card processing computer belonging to and located at the Village Pizza restaurant, Anacortes, WA, and obtained therefrom credit card track data that included credit card account numbers issued by Boeing Employees Credit Union or other financial institutions as defined by Title 18, United States Code, Section 20; and that they committed such offense in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States, specifically, bank fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii) and 2.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

COUNT 21

(Obtaining Information From a Protected Computer)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. Beginning on a date uncertain, but on or about August 9, 2010, and continuing until on or about February 23, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, they intentionally accessed a credit card processing computer belonging to and located at the Casa Mia Italian Pizzeria restaurant, Yelm, WA, and obtained therefrom credit card track data that included credit card account numbers issued by Boeing Employees Credit Union or other financial institutions as defined by Title 18, United States Code, Section 20; and that they committed such offense in furtherance of a criminal and tortious act in violation of the Constitution and laws of the United States, specifically, bank fraud, in violation of Title 18, United States Code, Section 1344.

All in violation of Title 18, United States Code, Sections 1030(a)(2) and 1030(c)(2)(B)(ii) and 2.

COUNT 22

(Possession of Fifteen or More Unauthorized Access Devices)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about January 20, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly and with intent to defraud, possessed fifteen or more unauthorized

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

access devices, that is, credit card account numbers that belonged to individuals who were customers of businesses located within the Western District of Washington, which credit card account numbers ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, stole from businesses, including the Broadway Grill, the Grand Central Baking Company, several Mad Pizza restaurants, Village Pizza, and Casa Mia Italian Pizzeria, located in the Western District of Washington, said possession affecting interstate and foreign commerce, in that the unauthorized access devices were possessed in order to market and sell them to others, for the intended purpose of making fraudulent purchases in multiple states within the United States, and foreign countries.

All in violation of Title 18, United States Code, Sections 1029(a)(3) and 1029(c)(1)(A)(i), and 2.

COUNT 23

(Trafficking in Unauthorized Access Devices)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. From on or about November 15, 2010, to on or about November 16, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly and with intent to defraud, trafficked in credit card track data, including credit card account numbers for credit card accounts that were established through and issued by the Boeing Employees Credit Union, in the Western District of Washington, and by such conduct, from on or about November 15, 2010, and ending on or about November 16, 2010, obtained profits aggregating approximately $83,490.00, said trafficking affecting interstate and foreign commerce, in that the credit card account numbers that were so trafficked were in turn

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

used to make fraudulent purchases in multiple states within the United States, and foreign countries.

All in violation of Title 18, United States Code, Sections 1029(a)(2) and 1029(c)(1)(A)(i), and 2.

COUNT 24

(Trafficking in Unauthorized Access Devices)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. From on or about January 31, 2011, to on or about February 1, 2011, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly and with intent to defraud, trafficked in credit card track data, including credit card account numbers for credit card accounts that were established through and issued by the Boeing Employees Credit Union, in the Western District of Washington, and by such conduct, from on or about January 31, 2011, and ending on or about February 1, 2011, obtained profits aggregating approximately $30,716.00, said trafficking affecting interstate and foreign commerce, in that the credit card account numbers that were so trafficked were in turn used to make fraudulent purchases in multiple states within the United States, and foreign countries.

All in violation of Title 18, United States Code, Sections 1029(a)(2) and 1029(c)(1)(A)(i), and 2.

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

COUNT 25

(Aggravated Identity Theft)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the personally identifiable credit card number of ****-****-****-5719, belonging to D.K., of Seattle, WA, within the Western District of Washington, during and in relation to a felony listed in Title 18, United States Code, Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code, Section 1344.

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

COUNT 26

(Aggravated Identity Theft)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the personally identifiable credit card number of ****-****-****-7089, belonging to N.S., of Seattle, WA, within the Western District of Washington, during and in relation to a felony listed in Title 18, United States Code,

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code, Section 1344.

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

COUNT 27

(Aggravated Identity Theft)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the personally identifiable credit card number of ****-****-****-0016, belonging to T.A., of Seattle, WA, within the Western District of Washington, during and in relation to a felony listed in Title 18, United States Code, Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code, Section 1344.

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

COUNT 28

(Aggravated Identity Theft)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the personally identifiable credit card number

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

of ****-****-****-0717, belonging to J.H., of Seattle, WA, within the Western District of Washington, during and in relation to a felony listed in Title 18, United States Code, Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code, Section 1344.

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

COUNT 29

(Aggravated Identity Theft)

1. Paragraphs 1 through 26 of Counts 1-5 are realleged and incorporated as if fully set forth herein.

2. On or about October 22, 2010, within the Western District of Washington and elsewhere, ROMAN SELEZNEV, aka TRACK2, aka ROMAN IVANOV, aka RUBEN SAMVELICH, aka nCuX, aka Bulba, aka bandysli64, aka smaus, aka Zagreb, aka shmak, knowingly transferred, possessed and used, without lawful authority, a means of identification of another person, to wit, the personally identifiable credit card number of ****-****-****-6316, belonging to L.S., of Seattle, WA, within the Western District of Washington, during and in relation to a felony listed in Title 18, United States Code,

//////////////////////////

//////////////////////////

//////////////////////////

//////////////////////////

//////////////////////////

//////////////////////////

//////////////////////////

//////////////////////////

//////////////////////////

//////////////////////////

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970

Section 1028A(c), to wit, Bank Fraud, in violation of Title 18, United States Code, Section 1344.

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

A TRUE BILL:

DATED:

Signature of the Foreperson redacted pursuant to the policy of the Judicial Conference

FOREPERSON

JENNY A. DURKAN
United States Attorney

Carl Blackstone
Assistant United States Attorney

Kathryn A. Warma
Assistant United States Attorney

UNITED STATES ATTORNEY
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
(206) 553-7970