


The Honorable Richard A. Jones

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.

October 8th 2014

WILLIAM M. McCOOL, Clerk

By  Deputy

UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON AT SEATTLE

UNITED STATES OF AMERICA,

Plaintiff

v.

ROMAN VALERYEVICH SELEZNEV,
aka ROMAN IVANOV,
aka RUBEN SAMVELICH,
aka BORIS SERGEYEVICH GRECHKIN,
aka ALEXEY DAVYDOV,
aka VALENTIN CHINAKOV,
aka JAMES CHOW,
aka ANDREY VMOTLA
aka MAXIM SALITOV,
aka IVAN IVANOV,
aka GARANIN EVGENIJ,
aka Track2,
aka smaus,
aka shmak,
aka nCuX,
aka Bulba,
aka 2pac,
aka JChow,
aka bandysli64,
aka boooksafe,
aka Zagreb,
aka Director,
aka Jareonii,

Defendant.

NO. CR11-0070RAJ

**SECOND SUPERSEDING
INDICTMENT**

1 The Grand Jury charges that:

2 **COUNTS 1-11**
3 **(Wire Fraud)**

4 **I. The Offense**

5 1. Beginning at a time unknown, but no later than February 13, 2007, and
6 continuing through on or about July 4, 2014, at Seattle, within the Western District of
7 Washington, and elsewhere, ROMAN SELEZNEV, aka ROMAN IVANOV, aka
8 RUBEN SAMVELICH, aka BORIS SERGEYEVICH GRECHKIN, aka ALEXEY
9 DAVYDOV, aka VALENTIN CHINAKOV, aka JAMES CHOW, aka ANDREY
10 VMOTLA, aka MAXIM SALITOV, aka IVAN IVANOV, aka GARANIN EVGENIJ,
11 aka Track2, aka smaus, aka shmak, aka nCuX, aka Bulba, aka 2pac, aka JChow, aka
12 bandysli64, aka boooksafe, aka Zagreb, aka Director, aka Jareni (hereinafter, ROMAN
13 SELEZNEV), and others known and unknown to the Grand Jury, with intent to defraud,
14 knowingly devised, a scheme and artifice to defraud and to obtain money and property by
15 means of materially false and fraudulent pretenses, representations and promises, as
16 further described below.

17 2. The object of the scheme and artifice to defraud was to obtain, market, and
18 sell stolen credit card numbers on underground websites for the purpose and with the
19 intent that the stolen credit card numbers would then in turn be used for fraudulent
20 transactions across the United States and in foreign countries, thereby defrauding the
21 issuing banks and the merchants that accepted the cards for payment based on the false
22 pretense that the users of the stolen credit card numbers were authorized users of those
23 credit card numbers. By way of this series of criminal actions, the defendant intended to
24 and did generate and receive millions of dollars in illicit profits, and caused millions of
25 dollars in losses to banks and merchants.

1 **II. Manner and Means of the Scheme and Artifice to Defraud**

2 **A. Defendant's Alias Names and Obfuscation Techniques**

3 3. It was part of the scheme and artifice to defraud that ROMAN SELEZNEV
4 concealed his identity through the use of several alias names and online nicknames
5 including, but not limited to: ROMAN IVANOV, RUBEN SAMVELICH, BORIS
6 SERGEYEVICH GRECHKIN, ALEXEY DAVYDOV, VALENTIN CHINAKOV,
7 JAMES CHOW, ANDREY VMOTLA, MAXIM SALITOV, IVAN IVANOV,
8 GARANIN EVGENIJ, Track2, smaus, shmak, nCuX, Bulba, 2pac, JChow, bandysli64,
9 boooksafe, Zagreb, Director, and Jareni.

10 4. It was further part of the scheme and artifice to defraud that ROMAN
11 SELEZNEV concealed his identity through the use of proxy servers and other
12 obfuscation techniques designed to hide his true identity and location while using
13 electronic mail and other online services to facilitate the scheme.

14 5. It was further part of the scheme and artifice to defraud that ROMAN
15 SELEZNEV, and others known and unknown to the Grand Jury, accepted payment for
16 stolen credit card data only by means of a limited number of payment services, including
17 services such as Bitcoin, Perfect Money, Paymer, Lesspay, eGold, Liberty Reserve, Web
18 Money, MoneyGram and Western Union, in an attempt to make it more difficult to trace
19 the proceeds of transactions and to conceal the identity of the parties.

20 **B. Defendant's Criminal Internet Infrastructure**

21 6. It was further part of the scheme and artifice to defraud that ROMAN
22 SELEZNEV, and others known and unknown to the Grand Jury, created and operated an
23 Internet-based infrastructure designed and intended to facilitate the theft, sale, and
24 fraudulent use of stolen credit card account numbers.

25 7. It was further part of the scheme and artifice to defraud that ROMAN
26 SELEZNEV, and others known and unknown to the Grand Jury, rented, configured, and
27 controlled servers in countries outside of the United States, including Ukraine and Russia,
28

1 that contained malware designed to infiltrate retail point of sale computer systems and to
2 steal credit card numbers (hereinafter “the malware servers”). The malware servers
3 included, but were not limited to, servers with the Internet addresses: “shmak.fvds.ru”
4 and “smaus.fvds.ru.” The malware on the malware servers included, but was not limited
5 to, malware denominated with the names “shmak,” “shmak2,” “kameo,” “hameo,”
6 “zameo,” “dte,” “dte2,” “dte4,” “dtca,” “rsca,” “remcomsvc,” and “perfectkeylogger.”

7 8. It was further part of the scheme and artifice to defraud that ROMAN
8 SELEZNEV, and others known and unknown to the Grand Jury, rented, configured, and
9 controlled servers, including servers in Ukraine and in McLean, Virginia, to receive and
10 compile the stolen credit card numbers (hereinafter the “dump collection servers”).

11 9. It was further part of the scheme and artifice to defraud that ROMAN
12 SELEZNEV, and others known and unknown to the Grand Jury, rented, configured, and
13 controlled servers in countries outside of the United States, including Ukraine, Russia and
14 Germany, for the purpose of hosting websites used to sell stolen credit card numbers,
15 including websites with the internet addresses: “nCuX.name,” “ncux.biz,” “ncux.asia,”
16 “ncuxlist.com,” “ncux.tv,” “track2.name,” “track2.cc,” track2.tv,” “track2vip.tv,”
17 “bulba.cc,” “secure.bulba.cc,” “secure.Track2.name,” and “2Pac.cc” (hereinafter in the
18 “dump shop servers”).

19 **C. The Computer Hacking and Theft of Credit Card Data**

20 10. It was further part of the scheme and artifice to defraud that ROMAN
21 SELEZNEV, and others known and unknown to the Grand Jury, developed and used
22 automated techniques, such as port scanning, to identify retail point of sale computer
23 systems, including computer systems within the Western District of Washington, that
24 were connected to the Internet, that were dedicated to or involved with credit card
25 processing, and that would be vulnerable to criminal hacks.

26 11. It was further part of the scheme and artifice to defraud that, once ROMAN
27 SELEZNEV, and others known and unknown to the Grand Jury, identified point of sale
28 computer systems that were vulnerable to criminal hacks, they issued commands to the

1 victim point of sale computers, including computers in the Western District of
2 Washington, that caused these victim computers to download malware from computer
3 servers they controlled.

4 12. It was further part of the scheme and artifice to defraud that ROMAN
5 SELEZNEV, and others known and unknown to the Grand Jury, configured the malware
6 that they downloaded onto the victims' computer systems to intercept credit card data
7 communicated between the victims' point of sale terminals and the victims' "back of the
8 house computers," that is, computers at the victim businesses that collect data from the
9 point of sale terminals.

10 13. It was further part of the scheme and artifice to defraud that ROMAN
11 SELEZNEV, and others known and unknown to the Grand Jury, configured the malware
12 to extract, copy, and compile the stolen credit card data and transmit the data from the
13 victim computer systems to the dump collection servers designated by ROMAN
14 SELEZNEV and others known and unknown to the Grand Jury.

15 14. It was further part of the scheme and artifice to defraud that, in some cases,
16 ROMAN SELEZNEV, and others known and unknown to the Grand Jury, also installed a
17 piece of software that would enable them easily to reconnect remotely to the victim
18 computer systems again, at a later date.

19 15. It was further part of the scheme and artifice to defraud that, after credit
20 card track data was transmitted from the hacked businesses, and compiled on the dump
21 collection servers ROMAN SELEZNEV and others known and unknown to the Grand
22 Jury controlled, ROMAN SELEZNEV and others known and unknown to the Grand Jury
23 would harvest the data and extract and segregate from it credit card account numbers,
24 Bank Identification Numbers ("BIN numbers"), and any other data possible, including
25 names of the account holders or PIN numbers, that would enhance the value of the data,
26 for sale to those who wished to use it for criminal, fraudulent purposes.

27 16. It was further part of the scheme and artifice to defraud that, using the same
28 or similar techniques to those described above, ROMAN SELEZNEV, and others known

1 and unknown to the Grand Jury, hacked into, installed malware on, and stole credit card
2 track data from, hundreds of retail businesses in the Western District of Washington and
3 elsewhere including, but not limited to: the Broadway Grill in Seattle, Washington;
4 Grand Central Baking Company in Seattle, Washington; four Mad Pizza locations in
5 Seattle and Tukwila, Washington; Village Pizza in Anacortes, Washington; Casa Mia
6 Italian Pizzeria restaurant in Yelm, Washington; Red Pepper Pizza in Duvall,
7 Washington; eighteen Extreme Pizza locations in California, Colorado, and Oregon;
8 fifteen Jet's Pizza locations in seven states; Schlotzky's Deli, in Coeur d'Alene, Idaho;
9 Days Jewelers in Waterville, Maine; Latitude Bar and Grill in New York, New York;
10 Grand Canyon Theater in Tusayan, Arizona; the Phoenix Zoo, in Phoenix, Arizona;
11 Mary's Pizza Shack, in Sonoma, California; City News Stand at multiple locations in
12 Illinois; and thirteen Z Pizza locations in California, Montana, and Virginia.

13 **D. The Marketing and Sale of Stolen Credit Card Data on Defendant's Websites**

14 17. It was further part of the scheme and artifice to defraud that, after ROMAN
15 SELEZNEV, and others known and unknown to the Grand Jury, had stolen, harvested,
16 and segregated the data that was valuable for sale, they posted and marketed that data for
17 sale on websites hosted on the dump shop servers, (hereinafter "the dump shop
18 websites"), including but not limited to those with the domain names: "nCuX.name,"
19 "ncux.biz," "ncux.asia," "ncuxlist.com," "ncux.tv," "track2.name," "track2.cc,"
20 track2.tv," "track2vip.tv," "bulba.cc," "secure.bulba.cc," "secure.Track2.name," and
21 "2Pac.cc."

22 18. It was further part of the scheme and artifice to defraud that ROMAN
23 SELEZNEV, and others known and unknown to the Grand Jury, operated different dump
24 shop websites at different times over the course of the scheme. Beginning at a date
25 uncertain, but no later than April 2009, and continuing through in or around October
26 2009, ROMAN SELEZNEV, and others known and unknown to the Grand Jury, operated
27 dump shop websites with the name "nCuX." Beginning in or around 2010 and
28 continuing through in or around January 2012, ROMAN SELEZNEV, and others known

1 and unknown to the Grand Jury, operated dump shop websites with the names "Track2"
2 and "Bulba." Beginning in or around January 2013, and continuing through on or about
3 July 4, 2014, ROMAN SELEZNEV, and others known and unknown to the Grand Jury,
4 operated a dump shop website with the name "2Pac."

5 19. It was further part of the scheme and artifice to defraud that when ROMAN
6 SELEZNEV, and others known and unknown to the Grand Jury, advertised and sold
7 stolen credit card numbers, BIN numbers, and related stolen data for sale on their dump
8 shop websites, they priced that data at varying levels, depending on its relative worth for
9 use in fraudulent transactions.

10 20. It was further part of the scheme and artifice to defraud that ROMAN
11 SELEZNEV, and others known and unknown to the Grand Jury, sought to attract and
12 entice customers to their dump shop websites by advertising "fresh dumps" of stolen
13 data, including, for example, an advertisement on November 24, 2010, as follows:

14 UPDATE OF 38,000 USA (TRACK1+2) AND 5.000 USD
15 TRACK2 ONLYTOTALLY MADE!!!
16 90% VALID! BIG BASE, NEW60 - TRACK1+TRACK2,
NEW61 - TRACK2 ONLY

17 and an advertisement on December 23, 2010, as follows:

18 UPDATE 17,000 FRESH DUMPS TOTALY MADE! VALID
19 VERY HIGH 95%!!
20 75% TRACK1 + TRACK2 AND OTHER TRACK2 ONLY!!!
21 Base - NEW65
22 Warning - today checker not work at all. Sorry for that.
23 Merry XMAS!:. THAT IS THE LAST UPDATE IN THIS YEAR. Hurry up to
fund account.

24 21. It was further part of the scheme and artifice to defraud that ROMAN
25 SELEZNEV, and others known and unknown to the Grand Jury, sought to enhance the
26 value and to spur sales of the stolen credit card data they marketed, for fraudulent use, by
27 offering a "checker" service through the dump shop websites, which, for a fee, would
28 enable customers to obtain instant validation information for the stolen credit card

1 numbers, and through which they also offered to “replace” numbers that were found to be
2 invalid.

3 22. It was further part of the scheme and artifice to defraud that, in order to
4 expand and maximize their customer base for stolen credit card numbers, ROMAN
5 SELEZNEV, and others known and unknown to the Grand Jury, advertised the dump
6 shop websites that they owned and controlled on various well-known carding forums
7 (that is, websites devoted to discussion of the trade of stolen credit card and other victim
8 data) such as “carder.su,” “crdsu.su,” “carder.biz,” “kuruapt.ru,” “omerta.cc,”
9 “infraud.cc,” “carderbase.su,” “crimes.ws,” “verified.cm,” “vor.cc,” and
10 “posdumps.com.”

11 23. It was further part of the scheme and artifice to defraud that, in order to
12 quash competition from other criminal carders, ROMAN SELEZNEV, and others known
13 and unknown to the Grand Jury, assumed total control and a monopoly over stolen credit
14 card sales made on the previously-established and preeminent carding forum “crdsu.su,”
15 in or around May of 2010.

16 24. It was further part of the scheme and artifice to defraud that ROMAN
17 SELEZNEV, and others known and unknown to the Grand Jury, solicited other criminals
18 engaged in the theft of credit card data to provide stolen credit card data, which ROMAN
19 SELEZNEV, and others known and unknown to the Grand Jury, then sold on dump shop
20 websites they operated and controlled, including the website “2Pac.cc,” to criminals
21 seeking to buy stolen credit card data.

22 25. It was further part of the scheme and artifice to defraud that ROMAN
23 SELEZNEV, and others known and unknown to the Grand Jury, posted advertisements
24 on carding forums on which they offered to resell credit card data stolen by others. For
25 example, on September 25, 2013, ROMAN SELEZNEV, and others known and unknown
26 to the Grand Jury, posted an advertisement on the carding forum omerta.cc stating:

27 2pac, the first market of dumps! All Sellers in once place!!! We invite
28 sellers, hackers and owners of dumps bases. You get the 50% share of

1 income from selling your base, that is much more than you can earn from
2 selling your base to other seller.

3 26. It was further part of the scheme and artifice to defraud that ROMAN
4 SELEZNEV, and others known and unknown to the Grand Jury, created and maintained
5 a website known as "posdumps.com" for the purpose of training potential purchasers of
6 stolen credit card data to use that data in fraudulent transactions, and for the additional
7 purpose of encouraging potential customers to buy credit card data from the website
8 2Pac.cc. For example, the posdumps.com website stated as follows:

9 This is tutorial [on] how to buy dumps and use in store (POS) (Make and
10 using fake credit card.) Here I will explain you how to earn money. From
11 \$500 to \$50,000 or even \$500,000. Remember this is illegal way! Process
12 from start to finish!

13 27. It was further part of the scheme and artifice to defraud that posdumps.com
14 educated potential purchasers in matters such as the equipment needed to encode
15 fraudulent credit cards with stolen card data, ways to obtain blank credit card templates,
16 and how to select and purchase "dumps" of stolen card data. Posdumps.com further
17 stated as follows:

18 You can buy dumps in online shop called 2pac.cc, that's the only one real
19 shop who is legit and they have dumps from almost all the world countries.
20 More than 1 million of stolen dumps.

21 The website further provided information on how to register at the 2pac.cc website and
22 how to pay for the stolen credit card data.

23 28. It was further part of the scheme and artifice to defraud that many
24 customers of the dump shops returned as repeat customers on numerous occasions to buy
25 stolen credit card data.

26 29. It was further part of the scheme and artifice to defraud that, in some
27 instances, ROMAN SELEZNEV used the stolen credit card data to make his own
28 fraudulent purchases.

1 30. It was further part of the scheme and artifice to defraud that ROMAN
2 SELEZNEV, and others known and unknown to the Grand Jury, stole, in total, over two
3 million credit card numbers, many of which they then sold through their dump shop
4 websites, nCuX.name, Track2.name, bulba.cc, and 2Pac.cc, thereby generating millions
5 of dollars of illicit profits for themselves.

6 31. It was further part of the scheme and artifice to defraud that the purchasers
7 of the stolen credit card numbers sold by ROMAN SELEZNEV, and others known and
8 unknown to the Grand Jury, then falsely represented themselves as authorized users of
9 the stolen credit cards and used the stolen credit card information to purchase goods and
10 services in fraudulent transactions throughout the United States and the world, including
11 over the Internet, resulting in millions of dollars in losses to, and thereby affecting,
12 merchants and banks, including financial institutions, as defined in Title 18, United States
13 Code, Section 20.

14 **E. Execution of the Scheme and Artifice to Defraud**

15 32. On or about the dates set forth below, at the locations set forth below,
16 within the Western District of Washington and elsewhere, for the purpose of executing
17 and attempting to execute this scheme and artifice to defraud, ROMAN SELEZNEV, and
18 others known and unknown to the Grand Jury, did knowingly transmit and cause to be
19 transmitted by wire communication in interstate and foreign commerce, writings, signs,
20 signals, pictures and sounds, each transmission of which constitutes a separate count of
21 this Second Superseding Indictment:

22 //

23 //

24

25

26

27

28

Count	Date	Wire Transmission
1	8/6/10	Transmission of malware from outside the State of Washington to computer belonging to Mad Pizza Madison Park in Seattle, Washington
2	8/7/10	Transmission of malware from outside the State of Washington to computer belonging to Mad Pizza First Hill in Seattle, Washington
3	8/9/10	Transmission of malware from outside the State of Washington to computer belonging to Casa Mia Italian Pizzeria restaurant in Yelm, Washington
4	8/28/10	Transmission of malware from outside the State of Washington to computer belonging to Mad Pizza South Lake Union in Seattle, Washington
5	10/4/10	Transmission of malware from outside the State of Washington to computer belonging to Grand Central Baking Company in Seattle, Washington
6	10/22/10	Transmission of malware from outside the State of Washington to computer belonging to Broadway Grill in Seattle, Washington
7	11/2/10	Transmission of malware from outside the State of Washington to computer belonging to Mad Pizza Starfire in Tukwila, Washington
8	12/15/10	Transmission of malware from outside the State of Washington to computer belonging to Mad Pizza South Lake Union in Seattle, Washington
9	12/23/10	Transmission of stolen credit card data from Village Pizza in Anacortes, Washington, to server controlled by defendant outside the State of Washington
10	1/10/11	Transmission of stolen credit card data from Mad Pizza Starfire in Tukwila, Washington, to server controlled by defendant outside the State of Washington
11	10/26/13	Transmission of malware from outside the State of Washington to computer belonging to Red Pepper Pizzeria in Duvall, Washington

The Grand Jury further alleges that the above violations each affected one or more financial institutions as defined in Title 18, United States Code, Section 20.

All in violation of Title 18, United States Code, Sections 1343 and 2.

//

//

COUNTS 12-20

(Intentional Damage to a Protected Computer)

1. Paragraphs 1 through 31 of Counts 1-11 are realleged and incorporated as if fully set forth herein.

2. On or about the dates set forth below, at the locations set forth below, within the Western District of Washington and elsewhere, ROMAN SELEZNEV 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 credit card processing computers belonging to the businesses set forth below, with each of the following incidents representing a separate count of this Second Superseding Indictment:

Count	Date	Victim
12	8/6/10	Mad Pizza Madison Park (Seattle)
13	8/7/10	Mad Pizza First Hill (Seattle)
14	8/9/10	Casa Mia Italian Pizzeria restaurant (Yelm)
15	8/28/10	Mad Pizza South Lake Union (Seattle)
16	9/13/10	Village Pizza (Anacortes)
17	10/4/10	Grand Central Baking Company (Seattle)
18	10/22/10	Broadway Grill (Seattle)
19	11/2/10	Mad Pizza Starfire (Tukwila)
20	10/26/13	Red Pepper Pizzeria (Duvall)

The Grand Jury further alleges that each incident charged above 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.

COUNTS 21-29**(Obtaining Information From a Protected Computer)**

1. Paragraphs 1 through 31 of Counts 1-11 are realleged and incorporated as if fully set forth herein.

2. On or about the dates set forth below, at the locations set forth below, within the Western District of Washington and elsewhere, ROMAN SELEZNEV intentionally accessed a computer without authorization, and thereby obtained information from a protected computer, to wit, ROMAN SELEZNEV intentionally accessed credit card processing computers belonging to and located at the businesses set forth below, and thereby obtained credit card track data, with each of the following incidents constituting a separate count of this Second Superseding Indictment:

Count	Begin Date	End Date	Victim
21	8/6/10	2/15/11	Mad Pizza Madison Park (Seattle)
22	8/7/10	2/15/11	Mad Pizza First Hill (Seattle)
23	8/9/10	2/23/11	Casa Mia Italian Pizzeria restaurant (Yelm)
24	8/28/10	2/1/11	Mad Pizza South Lake Union (Seattle)
25	9/13/10	3/26/11	Village Pizza (Anacortes)
26	10/4/10	12/1/10	Grand Central Baking Company (Seattle)
27	10/22/10	10/27/10	Broadway Grill (Seattle)
28	11/2/10	2/1/11	Mad Pizza Starfire (Tukwila)
29	10/26/13	5/1/14	Red Pepper Pizzeria (Duvall)

The Grand Jury further alleges that each of the offenses charged above was committed for purposes of commercial advantage and private financial gain and in furtherance of other criminal acts in violation of the laws of the United States, specifically access device fraud in violation of Title 18, United States Code, Sections 1029(a)(2) and (a)(3), and wire fraud in violation of Title 18, United States Code, Section 1343.

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

COUNTS 30-38

(Possession of Fifteen or More Unauthorized Access Devices)

1. Paragraphs 1 through 31 of Counts 1-11 are realleged and incorporated as if fully set forth herein.

2. On or about the dates set forth below, at the locations set forth below, within the Western District of Washington and elsewhere, ROMAN SELEZNEV knowingly, and with intent to defraud, possessed 15 or more unauthorized access devices, that is, credit card account numbers that belonged to individuals who were customers of the businesses identified below, which credit card account numbers ROMAN SELEZNEV stole from those businesses, said possession affecting interstate and foreign commerce. Each of the following incidents constitutes a separate count of this Second Superseding Indictment:

Count	Begin Date	End Date	Victim
30	8/6/10	2/15/11	Mad Pizza Madison Park (Seattle)
31	8/7/10	2/15/11	Mad Pizza First Hill (Seattle)
32	8/9/10	2/23/11	Casa Mia Italian Pizzeria restaurant (Yelm)
33	8/28/10	2/1/11	Mad Pizza South Lake Union (Seattle)
34	9/13/10	3/26/11	Village Pizza (Anacortes)
35	10/4/10	12/1/10	Grand Central Baking Company (Seattle)
36	10/22/10	10/27/10	Broadway Grill (Seattle)
37	11/2/10	2/1/11	Mad Pizza Starfire (Tukwila)
38	10/26/13	5/1/14	Red Pepper Pizzeria (Duvall)

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

COUNT 39

(Aggravated Identity Theft)

1
2
3 1. Paragraphs 1 through 31 of Counts 1-11 are realleged and incorporated as if
4 fully set forth herein.

5
6 2. On or about October 22, 2010, at Seattle, within the Western District of
7 Washington and elsewhere, ROMAN SELEZNEV knowingly transferred, possessed and
8 used, without lawful authority, a means of identification of another person, to wit, the
9 credit card number ****-****-****-5719, belonging to D.K, during and in relation to
10 felonies listed in Title 18, United States Code, Section 1028A(c), to wit, wire fraud, in
11 violation of Title 18, United States Code, Section 1343, and access device fraud in
12 violation of Title 18, United States Code, Sections 1029(a)(2) and (a)(3).

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

COUNT 40

(Aggravated Identity Theft)

14
15
16 1. Paragraphs 1 through 31 of Counts 1-11 are realleged and incorporated as if
17 fully set forth herein.

18 2. On or about April 9, 2014, at Duvall, within the Western District of
19 Washington and elsewhere, ROMAN SELEZNEV knowingly transferred, possessed, and
20 used, without lawful authority, a means of identification of another person, and did aid,
21 abet, counsel, command, induce and procure the transfer, possession and use, without
22 lawful authority, of a means of identification of another person, to wit, the personally
23 identifiable credit card number ****-****-****-2897, belonging to R.G., during and in
24 relation to felonies listed in Title 18, United States Code, Section 1028A(c), to wit, wire
25 fraud, in violation of Title 18, United States Code, Section 1343 and access device fraud
26 in violation of Title 18, United States Code, Sections 1029(a)(2) and (a)(3).

27 All in violation of Title 18, United States Code, Sections 1028A(a)(1) and 2.
28

FORFEITURE

1
2 1. The allegations contained in Counts 1-38 of this Second Superseding
3 Indictment are hereby realleged and incorporated by reference for the purpose of alleging
4 forfeitures to the United States pursuant to Title 18, United States Code, Sections
5 982(a)(2), 1029(c)(1)(C), and 1030(i)(1)(A) and (B).

6 2. Upon conviction of any of the offenses charged in Counts 1-11 above, in
7 violation of Title 18, United States Code, Section 1343, ROMAN SELEZNEV shall
8 forfeit to the United States of America, pursuant to Title 18, United States Code, Section
9 982(a)(2), any and all property, real or personal, that constitutes or is derived, directly or
10 indirectly, from proceeds traceable to the offense.

11 3. Upon conviction of any of the offenses charged in Counts 12-29 above, in
12 violation of Title 18, United States Code, Section 1030(a)(5)(A) and Title 18, United
13 States Code, Section 1030(a)(2), ROMAN SELEZNEV shall forfeit to the United States
14 of America, pursuant to Title 18, United States Code, Section 1030(i)(1)(A) and (B), any
15 personal property that was used or intended to be used to commit or to facilitate the
16 commission of the offenses and any property, real or personal, constituting or derived
17 from, any proceeds that defendant obtained, directly or indirectly, as a result of such
18 violations.

19 4. Upon conviction of any of the offenses charged in Counts 30-38, above, in
20 violation of Title 18, United States Code, Section 1029(a)(3), ROMAN SELEZNEV,
21 shall forfeit to the United States of America, pursuant to Title 18, United States Code,
22 Section 982(a)(2)(B), any and all property, real or personal, that constitutes or is derived,
23 directly or indirectly, from proceeds traceable to the offenses.

24 5. The property to be forfeited includes, but is not limited to the following:

25 a. **Money Judgment.** A sum of money representing the proceeds
26 obtained as a result of the offenses charged in Counts 1 - 38 of this Second Superseding
27 Indictment.

1 b. **Substitute Assets.** If any of the above described forfeitable
2 property, as a result of any act or omission of the Defendant:
3 i. cannot be located upon the exercise of due diligence;
4 ii. has been transferred or sold to, or deposited with, a third
5 party;
6 iii. has been placed beyond the jurisdiction of the Court;
7 iv. has been substantially diminished in value; or
8 v. has been commingled with other property which cannot be
9 subdivided without difficulty;
10 the United States of America shall be entitled to forfeiture of substitute property pursuant
11 to Title 21, United States Code, Section 853(p), as incorporated by Title 28, United States
12 Code, Section 2461(c).

13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

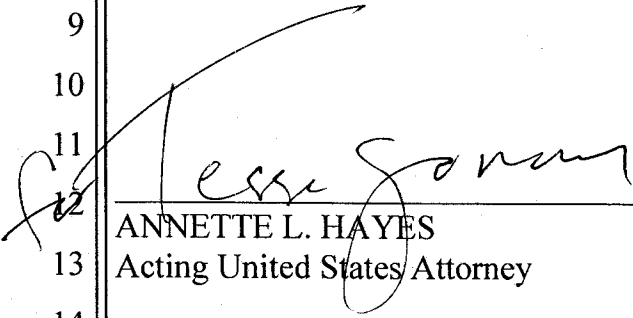
All pursuant to Title 18, United States Code, Sections 982(a)(2), 1029(c)(1)(C), and 1030(i)(1)(A) and (B).

A TRUE BILL:

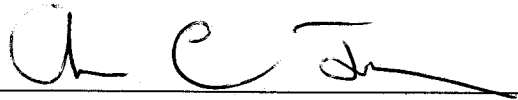
DATED:

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

FOREPERSON



ANNETTE L. HAYES
Acting United States Attorney



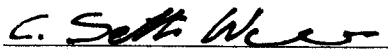
ANDREW C. FRIEDMAN
Assistant United States Attorney



NORMAN BARBOSA
Assistant United States Attorney



ETHAN ARENSON
Trial Attorney



SETH WILKINSON
Assistant United States Attorney