JUSTICE NEWS

Department of Justice

Office of Public Affairs

FOR IMMEDIATE RELEASE Friday, June 15, 2012

Alleged International Credit Card Trafficker “Badb” Extradited from France to the United States

WASHINGTON – Vladislav Anatolievich Horohorin, aka “BadB” of Moscow, an alleged international credit card trafficker thought to be one of the most prolific sellers of stolen credit card data, has been extradited from France to the United States to face criminal charges filed in the District of Columbia and in the Northern District of Georgia.

The extradition was announced today by Assistant Attorney General Lanny A. Breuer of the Justice Department’s Criminal Division, U.S. Attorney Ronald C. Machen Jr. for the District of Columbia, U.S. Attorney Sally Quillian Yates of the Northern District of Georgia, U.S. Secret Service (USSS) Assistant Director for Investigations David J. O’Connor, and Special Agent in Charge Brian D. Lamkin of the FBI’s Atlanta Field Office.

Horohorin, 27, made his first appearance before U.S. District Judge Ellen Segal Huvelle in the District of Columbia yesterday. He was extradited to the United States on June 6, 2012, and was arraigned before U.S. Magistrate Judge Alan Kay in the District of Columbia on June 7, 2012. He was ordered detained pending trial.

“According to the indictment, Mr. Horohorin was one of the most notorious credit card traffickers in the world, transacting in stolen credit information across the globe,” said Assistant Attorney General Breuer. “Due to our strong relationships with our international law enforcement partners, we secured his extradition to the United States, where he now faces multiple criminal counts in two separate indictments. We will continue to do everything we can to bring cybercriminals to justice, including those who operate beyond our borders.”

“Our indictment alleges that this young man used his technological savvy to profit by selling stolen credit card information over the Internet on a massive scale,” said U.S. Attorney Machen. “We are pleased that he has been extradited to the United States to face these criminal charges in a District of Columbia courtroom. This prosecution demonstrates that those who try to rip off Americans from behind a computer screen across an ocean will not escape American justice.”

“The Secret Service is committed to identifying and apprehending those individuals that continue to attack American financial institutions and we will continue to work through our international and domestic law enforcement partners in order to accomplish this,” said USSS Assistant Director O’Connor.

“International cyber criminals who target American citizens and businesses often believe they are untouchable because they are overseas,” said U.S. Attorney Yates. “But as this case demonstrates, we will work relentlessly with our law enforcement partners around the world to charge, find and bring those criminals to justice.”

“Horohorin’s extradition to the United States demonstrates the FBI’s expertise in conducting long-term investigations into complex criminal computer intrusions, resulting in bringing the most egregious cyber criminals to justice, even from foreign shores,” said Special Agent in Charge Lamkin. “The combined efforts of law enforcement agencies to include our international partners around the world will ensure this trend continues.”

Horohorin was indicted by a federal grand jury in the District of Columbia in November 2009 on charges of access device fraud and aggravated identity theft. In a separate investigation, a federal grand jury in the Northern District of Georgia returned a superseding indictment against

Horohorin in August 2010, charging him with conspiracy to commit wire fraud, wire fraud and access device fraud. In August 2010, French law enforcement authorities, working with the U.S. Secret Service, identified Horohorin in Nice, France, and arrested him as he was attempting to board a flight to return to Moscow.

According to the indictment filed in the District of Columbia, Horohorin was the subject of an undercover investigation by USSS agents. Horohorin, who is a citizen of Israel, Russia and Ukraine, allegedly used online criminal forums such as “CarderPlanet” and “carder.su” to sell stolen credit card information, known as “dumps,” to online purchasers around the world. According to the indictment, Horohorin, using the online name “BadB,” advertised the availability of stolen credit card information through these web forums and directed purchasers to create accounts at “dumps.name,” a fully-automated dumps vending website operated by Horohorin and hosted outside the United States. The website was designed to assist in the exchange of funds for the stolen credit card information. Horohorin allegedly directed buyers to fund their “dumps.name” account using funds transferred by services including “Webmoney,” an online currency service hosted in Russia. The purchaser would then access the “dumps.name” website and select the desired stolen credit card data. Using an online undercover identity, USSS agents negotiated the sale of numerous stolen credit card dumps.

According to the indictment filed in the Northern District of Georgia, Horohorin was one of the lead cashers in an elaborate scheme in which 44 counterfeit payroll debit cards were used to withdraw more than $9 million from over 2,100 ATMs in at least 280 cities worldwide in a span of less than 12 hours. Computer hackers broke into a credit card processor located in the Atlanta area, stole debit card account numbers, and raised the balances and withdrawal limits on those accounts while distributing the account numbers and PIN codes to lead cashers, like Hororhorin, around the world.

Horohorin faces a maximum penalty of 10 years in prison for each count of access device fraud, 20 years in prison for each count of conspiracy to commit wire fraud and wire fraud and a statutory consecutive penalty of two years in prison for the aggravated identity theft count.

The charges in the indictments are merely allegations and a defendant is presumed innocent until proven guilty.

The District of Columbia case is being prosecuted by Trial Attorneys Carol Sipperly, Ethan Arenson and Corbin Weiss of the Computer Crime and Intellectual Property Section (CCIPS) in the Justice Department’s Criminal Division. Weiss also serves as a Special Assistant U.S. Attorney for the District of Columbia. The District of Columbia case is being investigated by USSS. Key assistance was provided by the French Police Nationale Aux Frontiers and the Netherlands Police Agency National Crime Squad High Tech Crime Unit. The FBI Atlanta field office provided information helpful to the investigation.

The Northern District of Georgia case is being prosecuted by Assistant U.S. Attorneys Nick Oldham and Lawrence R. Sommerfeld and Trial Attorney Sipperly of CCIPS. The Atlanta case is being investigated by the FBI. Assistance was provided by numerous law enforcement partners. U.S. Secret Service provided information helpful to the investigation.

The Office of International Affairs in the Justice Department’s Criminal Division provided invaluable assistance.

12-767 Criminal Division

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

UNITED STATES OF AMERICA	:	**CRIMINAL NO.**
	:	
v.	:	**GRAND JURY ORIGINAL**
	:	
VLADISLAV ANATOLIEVICH HOROHORIN,	:	**VIOLATIONS:**
	:	
	:	**18 U.S.C. § 1029 (Access Device**
Defendant	:	**Fraud);**
	:	**18 U.S.C. § 1028A (Aggravated**
	:	**Identity Theft);**
	:	**18 U.S.C. § 2 (Aiding and Abetting and**
	:	**Causing an Act to be Done)**
	:	
	:	

INDICTMENT

The Grand Jury charges that:

At all times material to this Indictment:

Introduction

1. The term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds. A credit card number is an access device.

2. The term "unauthorized access device" means any access device that is lost, stolen, expired, revoked, canceled, or obtained with intent to defraud.

3. CarderPlanet and Carder.su are examples of organized criminal websites dedicated to promoting: malicious computer hacking; Internet fraud schemes; electronic theft of personal financial and identifying information; trafficking in and use of stolen credit card and debit card information (commonly referred to by criminals by the slang term "dumps"), stolen bank account information, and other stolen individual identifying information; and the production of, trafficking in, and use of counterfeit identification documents. The person using the alias "BadB" is a known trader of dumps.

4. Defendant, VLADISLAV ANATOLIEVICH HOROHORIN, is a citizen of Israel and the Ukraine.

5. Defendant, VLADISLAV ANATOLIEVICH HOROHORIN, used the alias "BadB" to operate an illegal business selling dumps (i.e., unauthorized access devices).

COUNT ONE
(Access Device Fraud)

6. The allegations set forth in paragraphs 1 through 5 of this Indictment are realleged and incorporated by reference herein.

7. Before on or about April 27, 2009, BadB posted an advertisement on the Internet carding forum *carder.su*. The advertisement listed BadB's title as "Seller of dumps." BadB advised in the advertisement that he had been selling dumps for approximately eight years, "since the days of CarderPlanet" (one of the original carding websites, which is now defunct). He also stated that he was one of the biggest dumps vendors on the market. BadB referred interested customers to his dumps vending websites *dumps.name* and *badb.biz,* and further advised that he could be contacted via the ICQ account number 49162552. "ICQ" is an Internet-based online chatting service.

8. On or about May 15, 2009, using an undercover computer located in the District of Columbia, a United States Secret Service (USSS) agent engaged in undercover communications with BadB via an ICQ account. BadB instructed to send funds via Western Union to the name Sergey Dubrovskih, X, Ukraine. BadB further advised that once the funds were received, the account established at *dumps.name*, would be funded within twelve hours. Using a Western Union location in Arlington, Virginia, USSS agents sent $1,250.00 in undercover funds as instructed.

9. On or about May 19, 2009, USSS agents accessed the *dumps.name* website, which is hosted outside the United States, and observed that the account had been credited with the undercover funds sent via Western Union. At that time, USSS agents purchased fifty-eight credit card dumps from BadB's website, for a total of approximately US $1,160. Several of the purchased dumps were subsequently verified by Visa to be authentic access devices.

10. On or about July 9, 2009, USSS agents again accessed *dumps.name* and observed that BadB was vending credit card dumps from a variety of different banks from countries throughout the world. Using an undercover computer located in the District of Columbia, USSS agents again engaged in undercover communications with BadB via ICQ for the purposes of purchasing credit card dumps from the *dumps.name* website. During these communications, BadB advised that he no longer accepted funds via Western Union and that all purchases must now be made via "WebMoney" through the *dumps.name* website. "WebMoney" is an online electronic payment system based in Moscow, Russia.

11. On or about July 10, 2009, USSS agents logged into the Internet website *www.planetwm.com*, an online currency exchange, for the purpose of converting the undercover funds to WebMoney. At the direction of *planetwm.com*, USSS agents, using a Western Union

location in Washington, DC, sent $1,246.00 in undercover funds to the name "Valentin Vladimirovich Ivanov" in X, Russia.

12. On or about July 17, 2009, USSS agents observed that the undercover WebMoney account number XXXXXXXXX2418 had been funded with the undercover funds sent via Western Union and *planetwm.com*. Using an undercover computer in the District of Columbia, USSS agents then used the undercover funds in the WebMoney account to establish a credit at *dumps.name*, which is hosted outside the United States. USSS agents then purchased thirteen credit card dumps, for a total of approximately US $1,163.

13. Defendant HOROHORIN knew that the access devices he sold were unauthorized (i.e., that they were credit card account numbers issued to other persons that were lost, stolen, expired, revoked, canceled, or obtained with intent to defraud). Defendant HOROHORIN sold the access devices with intent to defraud the legitimate cardholders and banks.

14. Between in or about May 2009 and in or about November 2009, in the District of Columbia and elsewhere, VLADISLAV ANATOLIEVICH HOROHORIN did knowingly and with intent to defraud aid and abet another in the possession of more than fifteen credit card account numbers issued to other persons that were lost, stolen, expired, revoked, canceled, or obtained with intent to defraud, which are unauthorized access devices, said activity affecting interstate commerce.

(Access Device Fraud, Aiding and Abetting and Causing and Act to be Done in violation of Title 18, United States Code, Sections 1029(a)(3), 2)

COUNT TWO
(Aggravated Identity Theft)

15. The allegations set forth in paragraphs 1 through 13 of this Indictment are realleged and incorporated by reference herein.

16. Between in or about May 2009 and in or about November 2009, in the District of Columbia and elsewhere, VLADISLAV ANATOLIEVICH HOROHORIN did knowingly transfer, without lawful authority, a means of identification of another person, specifically credit card account numbers belonging to others, during and in relation to access device fraud in violation of Title 18, United States Code, Section 1029(a)(3).

(Aggravated Identity Theft,
in violation of Title 18, United States Code, Sections 1028A(a)(1) and (c)(4))

A TRUE BILL

Foreperson

/s/
CHANNING D. PHILLIPS
ACTING UNITED STATES ATTORNEY

ORIGINAL

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF GEORGIA

ATLANTA DIVISION

UNITED STATES OF AMERICA	:	
	:	CRIMINAL INDICTMENT
v.	:	(Second Superseding)
	:	
VIKTOR PLESHCHUK,	:	
SERGEI TŠURIKOV,	:	NO. 1:09-CR-491
HACKER 3,	:	
OLEG COVELIN,	:	
IGOR GRUDIJEV,	:	
RONALD TSOI,	:	
EVELIN TSOI,	:	
MIHHAIL JEVGENOV,	:	
VLADISLAV HOROHORIN, and	:	
SONYA MARTIN,	:	
	:	
Defendants.	:	

THE GRAND JURY CHARGES THAT:

COUNT ONE
(Conspiracy to Commit Wire Fraud)

1. From at least on or about November 4, 2008, through at least on or about November 25, 2008, in the Northern District of Georgia and elsewhere, the Defendants, VIKTOR PLESHCHUK, SERGEI TŠURIKOV, HACKER 3, OLEG COVELIN, VLADISLAV HOROHORIN, and SONYA MARTIN, together with others known and unknown to the Grand Jury, did knowingly conspire to devise a scheme and artifice to defraud, and to obtain money and property, by means of material 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, certain signs, signals, and sounds, that is, to knowingly cause computer commands to be transmitted from outside of the United States to the computer network of RBS WorldPay in the Northern District of Georgia, and to knowingly conduct and cause to be conducted ATM withdrawals using fraudulently obtained prepaid payroll card numbers and PIN codes from ATM terminals outside of the State of Georgia that were processed on computers within the Northern District of Georgia, in violation of 18 U.S.C. § 1349.

BACKGROUND

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

(a) RBS WorldPay (RBSW) was headquartered in Atlanta, in the Northern District of Georgia. RBS WorldPay was a wholly owned subsidiary of Citizens Financial Group (CFG), a bank holding company as defined in the Federal Deposit Insurance Act.

(b) RBS WorldPay processes credit and debit card transactions on behalf of financial institutions. The transactions occur throughout the world and are processed by electronic means. RBS WorldPay's computer servers are located in the Northern District of Georgia.

(c) One of the services offered by RBS WorldPay is the processing of prepaid payroll card transactions. Prepaid payroll

cards are debit cards funded through direct deposits from card holders' employers. Prepaid payroll cards allow employers to pay their employees through direct deposits to prepaid payroll card accounts, instead of using paychecks or direct deposits into employees' bank accounts. Cash may be withdrawn by presenting the prepaid payroll card to an automated teller machine and entering the card's PIN code. Prepaid payroll cards may also be used to purchase goods and services from participating merchants. Transactions associated with these cards are processed by RBS WorldPay on behalf of its client financial institutions. Information related to these transactions is maintained by RBS WorldPay on the company's computer network.

(d) RBS WorldPay processes the transactions associated with prepaid debit cards issued by the following banks: RBS Citizens, N.A.; Palm Desert National Bank; The Bankcorp, Inc.; and First Bank of Delaware. Each of these issuing banks is federally insured. In addition to being a federally insured financial institution, RBS Citizens, N.A., is a member bank of the Federal Reserve System.

CHARGED CONSPIRATORS

3. (a) Defendant PLESHCHUK is a computer hacker who during the relevant time period resided in or around St. Petersburg, Russia. Based on Defendant TŠURIKOV's reconnaissance, Defendant PLESHCHUK manipulated the data on the RBS WorldPay computer network, with

support from Defendants TŠURIKOV, HACKER 3, COVELIN, and others. Defendant PLESHCHUK with the support of Defendant TŠURIKOV developed the method by which the conspirators reverse engineered Personal Identification Numbers (PINs) from the encrypted data on the RBS WorldPay computer network. Defendant PLESHCHUK, with assistance from Defendant TŠURIKOV, Defendant HACKER 3, and others, raised the limits on certain of the prepaid payroll cards. Defendant PLESHCHUK and Defendant TŠURIKOV accessed the RBS WorldPay computer network and observed the withdrawals taking place on the cards they fraudulently obtained and distributed, tracking the proceeds of the fraud. Overall, Defendant PLESHCHUK managed the activities on the RBS WorldPay computer database, including modification of withdrawal limits, locking the cards so that there could be no further withdrawals, and tracking the amounts withdrawn. With Defendant TŠURIKOV, Defendant PLESHCHUK deleted and attempted to delete information on the RBS WorldPay computer network.

(b) Defendant TŠURIKOV is a computer hacker who during the relevant time period resided in or around Tallinn, Estonia. TŠURIKOV was responsible for reconnaissance of the RBS WorldPay computer network and for support of other hacking activity. Defendant TŠURIKOV was contacted by Defendant COVELIN regarding vulnerabilities in the RBS WorldPay computer network. Defendant TŠURIKOV shared this information with Defendant PLESHCHUK.

Defendant TŠURIKOV acted as liaison, connecting the hackers who found vulnerabilities on the computer network with Defendant PLESHCHUK, who could better exploit them. With Defendant PLESHCHUK, Defendant TŠURIKOV deleted and attempted to delete information on the RBS WorldPay computer network. Defendant TŠURIKOV also managed his own cashing group and provided fraudulently obtained card numbers and PIN codes to his group within Estonia. Cashers are individuals who used the fraudulently obtained payroll cards and PIN codes to obtain cash from ATMs. Defendant TŠURIKOV helped coordinate the receipt and distribution of proceeds.

(c) Defendant HACKER 3 is a computer hacker who, in addition to his computer hacking activities in support of Defendants PLESHCHUK and TŠURIKOV, was responsible for managing the networks of cashers who used the fraudulently obtained payroll cards and PIN codes to obtain cash from ATMs on a coordinated time schedule. Defendant HACKER 3 distributed fraudulently obtained prepaid payroll cards and their respective PIN codes to casher networks around the world. Defendant HACKER 3 then managed the dividing of the proceeds and the distribution of cash from the cashers to other members of the scheme, including to Defendant PLESHCHUK, Defendant TŠURIKOV, and others.

(d) Defendant COVELIN is a computer hacker who during the relevant time period resided in or around Chişinău, Moldova.

Defendant COVELIN learned of the vulnerability in the RBS WorldPay computer network and provided the vulnerability (or "bug") to Defendant TŠURIKOV so that it could be exploited for financial gain. Defendants PLESHCHUK, TŠURIKOV, and HACKER 3 provided Defendant COVELIN a prepaid payroll card account number and associated PIN code, and raised the available funds on that account so COVELIN could make substantial withdrawals. COVELIN then distributed the account number and PIN code he was provided to others to fraudulently withdraw funds.

(e) Defendant HOROHORIN was a lead casher who fraudulently withdrew RBSW funds from ATM(s) in or around Moscow, Russia. Defendant HOROHORIN currently maintains Israeli and Ukranian passports.

(f) Defendant MARTIN was a casher who fraudulently withdrew RBSW funds from ATMs and who provided cards with fraudulently obtained RBSW account numbers to others in or around Chicago, Illinois.

MEANS AND MANNERS

4. It was part of the conspiracy that:

(a) Beginning on or about November 4, 2008, Defendants PLESHCHUK, TŠURIKOV, HACKER 3, and COVELIN, aided and abetted by each other and by others, gained unauthorized access from outside of the United States into the computer network of RBS WorldPay,

located in the Northern District of Georgia. To gain unauthorized access, they used a vulnerability in the RBS WorldPay computer network that was provided to Defendant TŠURIKOV by Defendant COVELIN.

(b) During the period of on or about November 4, 2008, through on or about November 8, 2008, Defendants PLESHCHUK, TŠURIKOV, and HACKER 3, obtained, without authorization, information from the RBS WorldPay computer network, including prepaid payroll card numbers and PIN codes.

(c) Defendants PLESHCHUK, TŠURIKOV, HACKER 3, and others distributed approximately 44 prepaid payroll card numbers and their respective PIN codes to networks of cashers. The lead cashers distributed the card numbers and PIN codes to individuals throughout the world, inside and outside of the United States. Of the 44 prepaid payroll card numbers distributed to the cashers, 42 of the numbers related to cards issued by Palm Desert National Bank.

(d) On or before November 8, 2008, Defendants PLESHCHUK and TŠURIKOV, aided and abetted by others including Defendant HACKER 3, gained unauthorized access to the RBS WorldPay computer network and modified the data, raising the amount of funds available on the prepaid payroll card numbers they had fraudulently obtained and distributed. Also, Defendants PLESHCHUK and TŠURIKOV, aided and abetted by others including Defendant HACKER 3, raised the limits

that could be withdrawn from automated teller machines on the prepaid payroll card numbers they had distributed.

(e) On or about November 7, 2008, Defendants PLESHCHUK, TŠURIKOV, and HACKER 3 provided Defendant COVELIN with a payroll debit card account number and associated PIN code, and raised the available balance on that account number.

(f) On or about November 8, 2008, Defendants PLESHCHUK and TŠURIKOV provided Defendant HOROHORIN with a payroll debit card account number xxxxxxxxxxx9488 and associated PIN code and raised the available balance on the account number to $200,000.00. This RBSW payroll debit card account number was only assigned to HOROHORIN.

(g) On or about November 8, 2008, Defendants PLESHCHUK, TŠURIKOV, HACKER 3, and COVELIN notified the cashers, including HOROHORIN and others, to whom they distributed the fraudulently obtained payroll debit card numbers and PIN codes, to begin withdrawing funds.

(h) On or about November 8, 2008, Defendant MARTIN obtained payroll debit account number xxxxxxxxxxx7662 and its associated PIN code. Using this information, Defendant MARTIN distributed cards containing the fraudulently obtained account number to others and fraudulently withdraw funds from ATM terminals in or around Chicago, Illinois.

(i) With the limits raised, in the next approximately twelve

hours at over 2,100 ATM terminals located in at least 280 cities around the world, including in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan, and Canada, cashers used approximately 44 payroll debit cards to complete withdrawals worth over $9 million in United States currency.

(j) RBSW records show that approximately $125,739.30 was withdrawn from RBSW payroll debit card account number xxxxxxxxxxxx9488, assigned to HOROHORIN.

(k) While the cashers withdrew the funds, Defendants PLESHCHUK and TŠURIKOV accessed the RBS WorldPay computer network without authorization and monitored the withdrawals.

(l) After the withdrawals were completed, Defendants PLESHCHUK and TŠURIKOV sent computer commands from outside the United States to the RBS WorldPay computer network in the Northern District of Georgia, that destroyed data and attempted to destroy data on the RBS WorldPay computer network in an effort to, among other things, conceal their unauthorized access and fraud.

(m) The cashers were permitted to retain a percentage of the funds they had obtained, typically between 30% and 50%. The cashers returned the balance of the funds to the hackers, including Defendants PLESHCHUK, TŠURIKOV, and HACKER 3, using means such as WebMoney accounts and Western Union.

All in violation of 18 U.S.C. § 1349.

COUNTS TWO THROUGH TEN
(Wire Fraud)

5. The allegations contained in paragraphs 2 through 4 are re-alleged and incorporated as if fully set forth in this paragraph.

6. On or about the dates set forth below, in the Northern District of Georgia and elsewhere, Defendants VIKTOR PLESHCHUK and SERGEI TŠURIKOV, aided and abetted by each other, by Defendants HACKER 3 and OLEG COVELIN, and by others whose identities are currently known and unknown to the Grand Jury, for the purpose of executing and attempting to execute the aforesaid scheme and artifice, such scheme and artifice having been devised and intended to be devised to defraud, and to obtain money and property, by means of materially false and fraudulent pretenses, representations, and promises, did knowingly cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain signs, signals, and sounds, that is, the Defendant listed in the table below, aided and abetted by the other Defendants and by others, did knowingly cause the following computer commands to be transmitted from outside of the United States to the computer network of RBS WorldPay in the Northern District of Georgia:

Count	Date	Defendant Sending Command	Computer Command (redacted)
2	Nov. 7, 2008	PLESHCHUK	select top 100 * from xxxxLogs where xxxxLogID>2550000 AND xxxxPAN IN ('xxxxxxxxxxxx1627','xxxxxxxxxxxx6968','xxxxxxxxxxx5341','xxxxxxxxxxxx6050','xxxxxxxxxxxx0336','xxxxxxxxxxx7540','xxxxxxxxxxxx7662','xxxxxxxxxxxx4809','xxxxxxxxxxxx1905','xxxxxxxxxxxx6257','xxxxxxxxxxx7597','xxxxxxxxxxxx7217','xxxxxxxxxxxx7399','xxxxxxxxxxxx5251','xxxxxxxxxxxx2861','xxxxxxxxxxx9075','xxxxxxxxxxxx1597','xxxxxxxxxxxx8980','xxxxxxxxxxxx3926','xxxxxxxxxxxx3964','xxxxxxxxxxxx5798','xxxxxxxxxxxx5100','xxxxxxxxxxxx1041','xxxxxxxxxxx1782','xxxxxxxxxxxx3364','xxxxxxxxxxxx0193','xxxxxxxxxxxx5010','xxxxxxxxxxxx2717','xxxxxxxxxxx8076','xxxxxxxxxxxx1992')

3	Nov. 7, 2008	PLESHCHUK	select top 100 * from xxxxxxxxxxTransaction where xxxxxxxxxxID>82300000 AND xxxxPAN IN ('xxxxxxxxxxxx1627','xxxxxxxxxxxx6968','xxxxxxxxx xxx5341','xxxxxxxxxxxx6050','xxxxxxxxxxxx0336','x xxxxxxxxxxx7540','xxxxxxxxxxxx7662','xxxxxxxxxxxx 4809','xxxxxxxxxxxx1905','xxxxxxxxxxxx6257','xxxx xxxxxxxx7597','xxxxxxxxxxxx7217','xxxxxxxxxxxx739 9','xxxxxxxxxxxx5251','xxxxxxxxxxxx2861','xxxxxxx xxxxx9075','xxxxxxxxxxxx1597','xxxxxxxxxxxx8980', 'xxxxxxxxxxxx3926','xxxxxxxxxxxx3964','xxxxxxxxxx xx5798','xxxxxxxxxxxx5100','xxxxxxxxxxxx1041','xx xxxxxxxxx1782','xxxxxxxxxxxx3364','xxxxxxxxxxxx0 193','xxxxxxxxxxxx5010','xxxxxxxxxxxx2717','xxxxx xxxxxxx8076','xxxxxxxxxxxx1992')
4	Nov. 7, 2008	PLESHCHUK	UPDATE Card SET ATMxxxxxLimit=500000,POSxxxxxLimit=500000,ATMxxxx xxxxx=500000, ATMxxxxxLimit2=500000,POSxxxxxLimit2=500000,ATMxx xxxxxxx2=500000 where xxxxPAN IN ('xxxxxxxxxxxx1627')

5	Nov. 7, 2008	PLESHCHUK	delete from xxxxLogs where xxxxLogID>2400000 and xxxxPAN in ('xxxxxxxxxxxx4809','xxxxxxxxxxxx3926','xxxxxxxxx xxx1041','xxxxxxxxxxxx5815','xxxxxxxxxxxx4912','x xxxxxxxxxxx9488','xxxxxxxxxxxx2840','xxxxxxxxxxx 3890') delete from xxxxxxxxxxTransaction where xxxxxxxxxxID>82000000 and xxxxPAN in ('xxxxxxxxxxxx4809','xxxxxxxxxxxx3926','xxxxxxxxx xxx1041','xxxxxxxxxxxx5815','xxxxxxxxxxxx4912','x xxxxxxxxxxx9488','xxxxxxxxxxxx2840','xxxxxxxxxxx 3890') UPDATE Card SET ATMxxxxxLimit=505,POSxxxxxLimit=505,ATMxxxxxxxxx= 505, ATMxxxxxLimit2=5000,POSxxxxxLimit2=5000,ATMxxxxxx xxx2=5000 where xxxxPAN in ('xxxxxxxxxxxx4809','xxxxxxxxxxxx3926','xxxxxxxxx xxx1041','xxxxxxxxxxxx5815','xxxxxxxxxxxx4912','x xxxxxxxxxxx9488','xxxxxxxxxxxx2840','xxxxxxxxxxx 3890')
6	Nov. 7, 2008	TŠURIKOV	select top 3 * from xxxxxxxxxxTransaction where xxxxPAN='xxxxxxxxxxxx5024' and xxxxxxxxxxDateTime > '11/01/2008'

7	Nov. 7, 2008	TŠURIKOV	select * from xxxxxxxxxxTransaction where xxxxPAN='xxxxxxxxxxxx5024' and xxxxxxxxxxxDateTime > '11/01/2008'
8	Nov. 8, 2008	TŠURIKOV	select xxxxxxxxxxxID,xxxxxxxxxxxDateTime,xxxxxxxxxAmount ,xxxxxxxxName,xxxxMerchxxxx,xxxxAddr,xxxxCity,xxx xState,xxxxZip,xxxxCounty from xxxxxxxxxxTransaction where xxxxPAN='xxxxxxxxxxxx0336' and xxxxxxxxxxxID>82300000
9	Nov. 8, 2008	TŠURIKOV	select xxxxxxxxxxxID,xxxxxxxxxxxDateTime,xxxxxxxxxAmount ,xxxxxxxxName,xxxxMerchxxxx,xxxxAddr,xxxxCity,xxx xState,xxxxZip,xxxxCounty from xxxxxxxxxxTransaction where xxxxPAN='xxxxxxxxxxxx0336' and xxxxxxxxxxxID>82300000
10	Nov. 8, 2008	TŠURIKOV	delete from xxxxLogs where xxxxxxxID>2400000 and xxxxPAN in ('xxxxxxxxxxxx0336')

All in violation 18 U.S.C. §§ 1343 and 2.

COUNT ELEVEN
(Conspiracy to Commit Computer Fraud)

7. The allegations contained in paragraphs 2 through 4 are re-alleged and incorporated as if fully set forth in this paragraph.

8. From in or about November 4, 2008 through at least in or about November 25, 2008, in the Northern District of Georgia and

elsewhere, Defendants VIKTOR PLESHCHUK, SERGEI TŠURIKOV, HACKER 3, and OLEG COVELIN, together with others known and unknown to the Grand Jury, did knowingly and wilfully conspire to: (a) knowingly cause the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally cause damage and attempt to cause damage without authorization to a protected computer, causing loss aggregating at least $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, in violation of 18 U.S.C. §§ 1030 (a)(5)(A) and 1030(b); (b) intentionally access a computer without authorization, and thereby obtain information contained in a financial record of a financial institution, and of a card issuer as defined in 15 U.S.C. § 1602(n), and from a protected computer, and the offense being committed for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349 and wire fraud in violation of 18 U.S.C. § 1343, and the value of the information obtained exceeding $5,000, in violation of 18 U.S.C. § 1030(a)(2); and (c) access a protected computer without authorization and by means of such conduct further the intended fraud and obtain value, specifically, prepaid payroll card numbers and PIN codes, and withdrawals from such prepaid

payroll card accounts exceeding US$9 million, in violation of 18 U.S.C. § 1030(a)(4), all in violation of 18 U.S.C. § 371.

OVERT ACTS

9. In furtherance of the conspiracy and to achieve the objects thereof, the conspirators committed the following various overt acts among others, in the Northern District of Georgia and elsewhere:

(a) Defendants PLESHCHUK and TŠURIKOV took the actions described in Counts Two through Ten, issuing computer commands from outside of the United States to the RBS WorldPay computer network in the Northern District of Georgia.

(b) On or about November 4, 2008, Defendant COVELIN provided Defendant TŠURIKOV with knowledge of a vulnerability on the RBS WorldPay computer network located in the Northern District of Georgia.

(c) On or about November 4, 2008, Defendant TŠURIKOV accessed without authorization the RBS WorldPay computer network located in the Northern District of Georgia.

(d) On or about November 5, 2008, Defendants PLESHCHUK, TŠURIKOV, and COVELIN accessed without authorization the RBS WorldPay computer network located in the Northern District of Georgia.

(e) On or about November 5, 2008, Defendant COVELIN provided

Defendant PLESHCHUK login information, including a password, to obtain access to a computer server on the RBS WorldPay computer network, located in the Northern District of Georgia.

(f) On or about November 7, 2008, Defendant PLESHCHUK obtained information from the RBS WorldPay computer network located in the Northern District of Georgia.

(g) On or about November 7, 2008, Defendant PLESHCHUK modified information on the RBS WorldPay computer network located in the Northern District of Georgia.

(h) On or about November 7, 2008, Defendant HACKER 3 transferred account numbers and PIN codes obtained from the RBS WorldPay computer network to casher networks for their subsequent use at ATMs.

(i) On or about November 7, 2008 Defendant COVELIN received an account number and PIN code obtained from the RBS WorldPay computer network.

(j) On or about November 8, 2008, Defendants PLESHCHUK and TŠURIKOV accessed without authorization the RBS WorldPay computer network located in the Northern District of Georgia.

(k) On or about November 8, 2008, Defendants PLESHCHUK and TŠURIKOV deleted and attempted to delete information from the RBS WorldPay computer network located in the Northern District of Georgia.

COUNT TWELVE
(Computer Intrusion Causing Damage)

10. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendants VIKTOR PLESHCHUK and SERGEI TŠURIKOV, aided and abetted by each other, by Defendants HACKER 3, and OLEG COVELIN, and by others known and unknown to the Grand Jury, knowingly caused the transmission of a program, information, code, and command, and, as a result of such conduct, intentionally caused damage and attempted to cause damage without authorization to a protected computer, causing loss aggregating at least $5,000 in value to at least one person during a one-year period from a related course of conduct affecting a protected computer, in violation of 18 U.S.C. §§ 1030(a)(5)(A), 1030(b), 1030(c)(4)(B), and 2.

COUNT THIRTEEN
(Computer Intrusion Obtaining Information)

11. On or about November 6, 2008, in the Northern District of Georgia and elsewhere, Defendants VIKTOR PLESHCHUK and SERGEI TŠURIKOV, aided and abetted by Defendants HACKER 3 and OLEG COVELIN, and by others known and unknown to the Grand Jury, intentionally accessed a computer without authorization, and thereby obtained information contained in a financial record of a financial institution, and of a card issuer as defined in 15 U.S.C. § 1602(n), and from a protected computer, and the offense being

committed for purposes of commercial advantage and private financial gain, and in furtherance of a criminal and tortious act in violation of the Constitution and the laws of the United States, specifically, conspiracy to commit wire fraud in violation of 18 U.S.C. § 1349 and wire fraud in violation of 18 U.S.C. § 1343, and the value of the information obtained exceeding $5,000, in violation of 18 U.S.C. §§ 1030(a)(2), 1030(c)(2)(B)(i), 1030(c)(2)(B)(ii), 1030(c)(2)(B)(iii), and 2.

COUNT FOURTEEN
(Computer Intrusion Furthering Fraud)

12. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendants VIKTOR PLESHCHUK, SERGEI TŠURIKOV, and HACKER 3, aided and abetted by Defendant OLEG COVELIN and by others known and unknown to the Grand Jury, knowingly and with intent to defraud accessed a protected computer without authorization and by means of such conduct furthered the intended fraud and obtained value, specifically, prepaid payroll card numbers and PIN codes, and withdrawals from such prepaid payroll card accounts exceeding $9 million, in violation of 18 U.S.C. §§ 1030(a)(4), 1030(c)(3)(A), and 2.

COUNT FIFTEEN
(Aggravated Identity Theft)

13. On or about November 7, 2008, in the Northern District of Georgia and elsewhere, Defendants VIKTOR PLESHCHUK, SERGEI TŠURIKOV, and HACKER 3, aided and abetted by each other, by Defendant OLEG COVELIN, and by others known and unknown to the Grand Jury, during and in relation to the crime of wire fraud in violation of 18 U.S.C. § 1343, did knowingly transfer, possess, and use, without lawful authority, means of identification of other persons, that is, the Defendants knowingly transferred prepaid payroll card account numbers and associated PIN codes from the RBS WorldPay computer network located in the Northern District of Georgia, possessed the card account numbers and PIN codes, and transferred card account numbers and PIN codes to others for their use at ATM terminals, in violation of 18 U.S.C. §§ 1028A(a)(1), 1028A(b), 1028A(c)(5), and 2.

COUNT SIXTEEN
(Access Device Fraud)

14. The allegations contained in paragraphs 2 through 4, and paragraph 9, are re-alleged and incorporated as if fully set forth in this paragraph.

15. On or about November 8, 2008, Defendant SERGEI TŠURIKOV distributed fraudulently obtained prepaid payroll card numbers and PIN codes to Defendant IGOR GRUDIJEV, who, in turn, distributed the

information to Defendants RONALD TSOI, EVELIN TSOI, and MIHHAIL JEVGENOV in Estonia. Together, Defendants RONALD TSOI, EVELIN TSOI, and MIHHAIL JEVGENOV withdrew funds worth approximately US$289,000 from ATMs in Tallinn, Estonia. These transactions were debited on prepaid payroll card accounts on the RBS WorldPay computer system located in the Northern District of Georgia.

16. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendants RONALD TSOI, EVELIN TSOI, and MIHHAIL JEVGENOV, aided and abetted by Defendant IGOR GRUDIJEV and by others known and unknown to the Grand Jury, knowingly and with intent to defraud effected transactions with at least one access device issued to another person, that is prepaid payroll card account numbers and PIN codes which can be used, alone and in conjunction with another access device, to obtain money, goods, services, and other things of value, and that can be used to initiate a transfer of funds not originated solely by paper instrument, in order to receive payment and other things of value within a one year period the aggregate of value of which was at least $1,000, said offense affecting interstate and foreign commerce, in violation of 18 U.S.C. §§ 1029(a)(5), 1029(c)(1)(A)(ii), and 2.

COUNTS SEVENTEEN THROUGH TWENTY-ONE
(Wire Fraud)

17. The allegations contained in paragraphs 2 through 4 are re-alleged and incorporated as if fully set forth in this paragraph.

18. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendant HOROHORIN for the purpose of executing and attempting to execute the aforesaid scheme and artifice, such scheme and artifice having been devised and intended to be devised to defraud, and to obtain money and property, by means of materially false and fraudulent pretenses, representations, and promises, did knowingly cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain signs, signals, and sounds, that is, the Defendant knowingly caused wires signaling the following requests for the withdrawal of funds from fraudulently obtained RBSW prepaid payroll card account number xxxxxxxxxxxx9488 to be transmitted from outside of the United States to the computer network of RBSW in the Northern District of Georgia:

Count	Time (at or about, Moscow, Russia)	Amount (U.S.D.)
17	16:02:07	$370.04
18	16:02:46	$370.04
19	16:03:29	$370.04
20	16:04:08	$370.04
21	16:04:49	$370.04

All in violation 18 U.S.C. §§ 1343 and 2.

COUNT TWENTY-TWO
(Access Device Fraud)

19. The allegations contained in paragraphs 2 through 4 are re-alleged and incorporated as if fully set forth in this paragraph.

20. On or about November 8, 2008, Defendant HOROHORIN fraudulently obtained a prepaid payroll card associated with RBSW account number xxxxxxxxxxx9488 and associated PIN code from which funds worth at least $125,739.30 were withdrawn from ATMs in or around Moscow, Russia. These transactions were debited on prepaid payroll card accounts on the RBSW computer system located in the Northern District of Georgia.

21. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendant HOROHORIN aided and abetted by others known and unknown to the Grand Jury, knowingly and with intent to defraud effected transactions with at least one access device issued to another person, that is prepaid payroll card account numbers and PIN codes which can be used, alone and in conjunction with another access device, to obtain money, goods, services, and other things of value, and that can be used to initiate a transfer of funds not originated solely by paper instrument, in order to receive payment and other things of value within a one year period the aggregate of value of which was at least $1,000, said offense affecting interstate and foreign commerce, in violation of 18 U.S.C. §§ 1029(a)(5), 1029(c)(1)(A)(ii), and 2.

COUNTS TWENTY-THREE THROUGH TWENTY-EIGHT
(Wire Fraud)

17. The allegations contained in paragraphs 2 through 4 are re-alleged and incorporated as if fully set forth in this paragraph.

18. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendant SONYA MARTIN for the purpose of executing and attempting to execute the aforesaid scheme and artifice, such scheme and artifice having been devised and intended to be devised to defraud, and to obtain money and property, by means of materially false and fraudulent pretenses, representations, and promises, did knowingly cause to be transmitted in interstate and foreign commerce, by means of a wire communication, certain signs, signals, and sounds, that is, the Defendant knowingly caused wires signaling the following requests for the withdrawal of funds from fraudulently obtained RBSW prepaid payroll card account number xxxxxxxxxxxx7662 to be transmitted from in or around Chicago, Illinois, to the computer network of RBSW in the Northern District of Georgia:

Count	Time (at or about, Chicago, IL)	Amount (U.S.D.)
23	01:34:08	$803.00
24	01:35:09	$803.00
25	02:00:24	$803.00
26	04:33:00	$803.00
27	04:34:02	$803.00
28	04:35:11	$803.00

All in violation 18 U.S.C. §§ 1343 and 2.

COUNT TWENTY-NINE
(Access Device Fraud)

22. On or about November 8, 2008, in the Northern District of Georgia and elsewhere, Defendant SONYA MARTIN, aided and abetted by others known and unknown to the Grand Jury, knowingly and with intent to defraud trafficked in and used at least one unauthorized access device, that is prepaid payroll card account numbers and PIN codes which can be used, alone and in conjunction with another access device, to obtain money, goods, services, and other things of value, and that can be used to initiate a transfer of funds not originated solely by paper instrument, and during a one-year period by such conduct obtained anything of value aggregating at least $1,000, said offense affecting interstate and foreign commerce, in violation of 18 U.S.C. §§ 1029(a)(2), 1029(c)(1)(A)(i), and 2.

FORFEITURE

23. As a result of committing an offense as alleged in Counts 1-14 and 16-29 of this Indictment, the Defendants shall forfeit to the United States pursuant to Title 18, United States Code, Section 982(a)(2) any property, real or personal, which constitutes or is derived from proceeds obtained directly or indirectly, as the result of said offenses as alleged in this Indictment, including, but not limited to a sum of money representing the amount of

proceeds obtained as a result of the offense, of at least $9,477,146.67 in United States currency.

In addition, as a result of an offense as alleged in Counts 16, 22, and 29 of this Indictment, the Defendants shall forfeit to the United States pursuant to Title 18, United States Code, Section 1029(c) any personal property used or intended to be used to commit the offense(s).

If any of the above-described forfeitable property, as a result of any act or omission of the defendant(s):

(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 21 U.S.C. § 853(p) as incorporated by 18 U.S.C. § 982(b), to seek forfeiture of

any other property of said defendant(s) up to the value of the forgettable property described above.

A TRUE BILL

FOREPERSON

SALLY QUILLIAN YATES
UNITED STATES ATTORNEY

LAWRENCE R. SOMMERFELD
ASSISTANT UNITED STATES ATTORNEY
Georgia Bar Number 666936

NICHOLAS OLDHAM
ASSISTANT UNITED STATES ATTORNEY
Georgia Bar Number 592701

HOWARD W. COX
ASSISTANT DEPUTY CHIEF
COMPUTER CRIME & INTELLECTUAL PROPERTY SECTION
U.S. DEPARTMENT OF JUSTICE
D.C. Bar Number 222976

600 U.S. Courthouse
75 Spring Street, S.W.
Atlanta, GA 30303
Telephone 404-581-6000