Department of Justice

United States Attorney Sally Quillian Yates
Northern District of Georgia

FOR IMMEDIATE RELEASE
08/06/10
http://www.justice.gov/usao/gan/

CONTACT: F. Gentry Shelnutt
(404)581-6008
FAX (404)581-6160

INTERNATIONAL HACKER ARRAIGNED AFTER EXTRADITION

Elaborate Scheme Stole over $9.4 Million from Credit Card Processor

ATLANTA, GA - SERGEI TŠURIKOV, 26, of Tallinn, Estonia, has been extradited to the United States. TŠURIKOV appeared today and was arraigned before United States Magistrate Judge E. Clayton Scofield III, on federal charges of conspiracy to commit wire fraud, wire fraud, conspiracy to commit computer fraud, computer fraud, and aggravated identity theft. TŠURIKOV was indicted by a federal grand jury on these charges on November 10, 2009, along with VIKTOR PLESHCHUK, 29, of St. Petersburg, Russia, OLEG COVELIN, 29, of Chişinău, Moldova, and an unidentified individual. The indictment also charged IGOR GRUDIJEV, 32, RONALD TSOI, 32, EVELIN TSOI, 21, and MIHHAIL JEVGENOV, 34, each of Tallinn, Estonia, with access device fraud offenses.

United States Attorney Sally Quillian Yates said of the case, "In November 2008, in just one day, an American credit card processor was hacked in perhaps the most sophisticated and organized computer fraud attack ever conducted. Almost exactly one year later, the leaders of this attack were charged. With cooperation from law enforcement partners around the world, and most particularly in Estonia, we have now extradited to Atlanta one of the leaders of this ring.. This success would not have been possible without the efforts of the victim, and unprecedented cooperation from various law enforcement agencies worldwide."

"Computer hackers who steal from American financial networks must be held accountable for their crimes, whether they operate here or abroad," said Assistant Attorney General Breuer. "The Department of Justice, working hand in hand with our international law enforcement partners, is committed to denying these criminals safe haven outside the United States and will vigorously investigate and prosecute these crimes."

Atlanta FBI Special Agent in Charge Brian D. Lamkin stated, "Complex cyber based criminal investigations such as this are becoming all too prevalent. The advances in technology, while aiding the corporate world and the consumer, also aid the criminal in conducting well coordinated fraud or theft based schemes, often across international borders. The FBI extends its gratitude to those international partners who not only assisted with this investigation but with the extradition to the U.S. of one of its chief ring leaders in this multimillion dollar, multi-national theft ring."

According to United States Attorney Yates, the charges and other information presented in court: During November 2008, PLESHCHUK, TŠURIKOV, and COVELIN allegedly obtained unauthorized access into the computer network of "RBS WorldPay," the U.S. payment processing division of the Royal Bank of Scotland Group PLC, located in Atlanta. The indictment alleges that the group used sophisticated hacking techniques to compromise the data encryption that was used by RBS WorldPay to protect customer data on payroll debit cards. Payroll debit cards are used by various companies to pay their employees. By using a payroll debit card, employees are able to withdraw their regular salaries from an ATM.

Once the encryption on the card processing system was compromised, the hacking ring allegedly raised the account limits on compromised accounts, and then provided a network of "cashers" with 44 counterfeit payroll debit cards, which were used to withdraw more than $9 million from over 2,100 ATMs in at least 280 cities worldwide, including cities in the United States, Russia, Ukraine, Estonia, Italy, Hong Kong, Japan and Canada. The $9 million loss occurred within a span of less than 12 hours.

The hackers then allegedly sought to destroy data stored on the card processing network in order to conceal their hacking activity. The indictment alleges that the "cashers" were allowed to keep 30 to 50 percent of the stolen funds, but transmitted the bulk of those funds back to TŠURIKOV, PLESHCHUK and other co-defendants, using means such as WebMoney accounts and Western Union. Upon discovering the unauthorized activity, RBS WorldPay immediately reported the breach, and has substantially assisted in the investigation.

Throughout the duration of the cashout, PLESHCHUK and TŠURIKOV allegedly monitored the fraudulent ATM withdrawals in real-time from within the computer systems of RBS WorldPay. Once the withdrawals were completed, PLESHCHUK and TŠURIKOV allegedly attempted to conceal their activities in the RBS WorldPay computer network by destroying and attempting to destroy data.

TŠURIKOV was not only an alleged hacker, but also distributed fraudulently obtained debit card account numbers and PIN codes to IGOR GRUDIJEV, who, in turn, allegedly distributed the information to Defendants RONALD TSOI, EVELIN TSOI, and MIHHAIL JEVGENOV in Estonia. Together, RONALD TSOI, EVELIN TSOI, and

MIHHAIL JEVGENOV allegedly withdrew funds worth approximately $289,000 in U.S. funds from ATMs in Tallinn, Estonia.

The indictment contains sixteen counts. Count One charges PLESHCHUK, TŠURIKOV, COVELIN, and a fourth unidentified individual of conspiracy to commit wire fraud. Counts Two through Ten are substantive wire fraud charges brought against PLESHCHUK and TŠURIKOV, aided and abetted by COVELIN and the unidentified hacker, based on the computer commands sent from outside the United States to the computer network of RBS WorldPay in the Northern District of Georgia. Count Eleven charges PLESHCHUK, TŠURIKOV, COVELIN, and the fourth individual with conspiracy to commit computer fraud. Counts Twelve through Fourteen are substantive charges of computer fraud against the defendants. Count Fifteen charges these defendants with aggravated identity theft based on the prepaid payroll card account numbers and associated PIN codes they transferred, possessed, and used without authorization in committing the wire fraud. Count Sixteen charges RONALD TSOI, EVELIN TSOI, and JEVGENOV, aided and abetted by GRUDIJEV, with access device fraud.

The indictment seeks forfeiture of over $9.4 million of proceeds of the crimes from the defendants.

PLESHCHUK, TŠURIKOV, COVELIN, and the unidentified defendant each face a maximum sentence of up to 20 years for conspiracy to commit wire fraud and each wire fraud count; up to 5 years for conspiracy to commit computer fraud; up to 5 or 10 years for each count of computer fraud; a 2 year mandatory minimum for aggravated identity theft; and fines up to $3.5 million dollars. The charges against GRUDIJEV, the TSOI's, and JEVGENOV carry a maximum of up to 15 years incarceration for each count and a fine of up to $250,000. In determining the actual sentence, the Court will consider the United States Sentencing Guidelines, which are not binding but provide appropriate sentencing ranges for most offenders.

The early detection of fraudulent ATM withdrawal activities in Tallinn, Estonia led to an immediate response by the Estonian Central Criminal Police. Their investigative efforts led to the prompt identification of TŠURIKOV, GRUDIJEV, the TSOIs, and JEVGENOV. Cooperation between the Hong Kong Police Force and the FBI also led to a parallel investigation, resulting in the identification and arrest of two individuals who were responsible for withdrawing RBS WorldPay funds from ATM terminals in Hong Kong. The Netherlands Police Agency National Crime Squad High Tech Crime Unit and the Netherlands National Prosecutor's Office provided key assistance in the investigation.

Since the United States indictment was announced in November 2009, TŠURIKOV, GRUDIJEV, the TSOI's, and JEVGENOV have been convicted in Estonia

of fraud relating to ATM withdrawals. TŠURIKOV has now been extradited from Estonia to the United States to answer to the charges in the United States' indictment.

Members of the public are reminded that the indictment contains only allegations. A defendant is presumed innocent of the charges and it will be the government's burden to prove a defendant's guilt beyond a reasonable doubt at trial.

This case is being investigated by Special Agents of the Federal Bureau of Investigation. Assistance was provided by international law enforcement partners. The United States Secret Service also participated in the investigation. RBS World Pay immediately reported the crime and has substantially assisted in the investigation.

Assistant United States Attorneys Lawrence R. Sommerfeld and Gerald Sachs, and Assistant Deputy Chief Howard Cox of the Computer Crime and Intellectual Property Section of the U.S. Department of Justice are prosecuting the case. Senior Trial Attorney Deborah Gaynus of the Criminal Division's Office of International Affairs assisted with the extradition. Assistance was also provided by Senior Trial Attorneys Betsy Burke and Judith Friedman and Trial Attorneys Blair Berman and Roman Chaban of the Office of International Affairs.

For further information please contact Sally Q. Yates, United States Attorney, or F. Gentry Shelnutt, Criminal Chief, through Chris Koebrich at (404) 581-6008. The Internet address for the HomePage for the U.S. Attorney's Office for the Northern District of Georgia is www.usdoj.gov/usao/gan.