



Department of Justice

ACTING UNITED STATES ATTORNEY, SALLY QUILLIAN YATES
Northern District of Georgia

FOR IMMEDIATE RELEASE

11/10/09

<http://www.usdoj.gov/usao/gan/>

CONTACT: Patrick Crosby

(404)581-6016

FAX (404)581-6160

INTERNATIONAL EFFORT DEFEATS MAJOR HACKING RING

Elaborate Scheme Stole over \$9.4 Million from Credit Card Processor

Atlanta, GA - VIKTOR PLESHCHUK, 28, of St. Petersburg, Russia; SERGEI TŠURIKOV, 25, of Tallinn, Estonia; and OLEG COVELIN, 28, of Chişinău, Moldova, along with an unidentified individual, have been indicted by a federal grand jury on charges of conspiracy to commit wire fraud, wire fraud, conspiracy to commit computer fraud, computer fraud, and aggravated identity theft. IGOR GRUDIJEV, 31, RONALD TSOI, 31, EVELIN TSOI, 20, and MIHHAIL JEVGENOV, 33, each of Tallinn, Estonia, have been indicted by a federal grand jury on charges of access device fraud.

Acting United States Attorney Sally Quillian Yates said of the case, “Last November, in just one day, an American credit card processor was hacked in perhaps the most sophisticated and organized computer fraud attack ever conducted. Today, almost exactly one year later, the leaders of this attack have been charged. This investigation has broken the back of one of the most sophisticated computer hacking rings in the world. This success would not have been possible without the efforts of the victim, and unprecedented cooperation from various law enforcement agencies worldwide.”

In Washington, D.C., Assistant Attorney General of the Criminal Division Lanny A. Breuer said, “The charges brought against this highly sophisticated international hacking ring were possible only because of unprecedented international cooperation with our law enforcement partners, particularly between the United States and Estonia. Through our close cooperation, both nations have demonstrated our commitment to identifying sophisticated attacks on U.S. financial networks that are directed and operated from overseas and our commitment to bringing the perpetrators to justice.”

FBI Atlanta Special Agent in Charge Greg Jones said, “Through the diligent efforts of the victim company and multiple law enforcement agencies within the United States and around the world, the leaders of a technically advanced computer hacking group were identified and indicted in Atlanta, sending a clear message to cyber-criminals across the globe. Justice will not stop at international borders but continue with the on-

going cooperation between the FBI and other agencies such as the Estonian Central Criminal Police and the Netherlands Police Agency.”

According to Acting 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 TSURIKOV, 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. Charges based on these transactions are pending in Estonia.

The indictment charges 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. TŠURIKOV is presently in custody in Estonia on charges related to access device fraud. The extradition of TŠURIKOV to the United States is currently in process. Access device fraud charges are also pending in Estonia against GRUDIJEV, the TSOI's, 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.

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 Senior Counsel Kimberly Kiefer Peretti of the Computer Crime and Intellectual Property Section of the U.S. Department of Justice are prosecuting the case. Office of International Affairs counsel Deborah Gaynus is assisting with extradition matters. Treaty assistance was provided by Office of International Affairs counsels Betsy Burke, Blair Berman, Roman Chaban, Judith Friedman, Deborah Gaynus, Linda McKinney, and Mary McLaren.

For further information please contact Sally Q. Yates, Acting United States Attorney, or Charysse L. Alexander, Executive Assistant United States Attorney, through Patrick Crosby, Public Affairs Officer, U.S. Attorney's Office, at (404) 581-6016. 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.