Department of Justice

FOR IMMEDIATE RELEASE
Tuesday, August 5, 2008
WWW.USDOJ.GOV

AG
(202) 514-2007
TDD (202) 514-1888

Retail Hacking Ring Charged for Stealing and Distributing Credit and Debit Card Numbers from Major U.S. Retailers

More Than 40 Million Credit and Debit Card Numbers Stolen

BOSTON – Eleven perpetrators allegedly involved in the hacking of nine major U.S. retailers and the theft and sale of more than 40 million credit and debit card numbers have been charged with numerous crimes, including conspiracy, computer intrusion, fraud and identity theft, Attorney General Michael B. Mukasey, U.S. Attorney for the District of Massachusetts Michael J. Sullivan, U.S. Attorney for the Southern District of California Karen P. Hewitt, U.S. Attorney for the Eastern District of New York Benton J. Campbell and U.S. Secret Service Director Mark Sullivan announced today. The scheme is believed to constitute the largest hacking and identity theft case ever prosecuted by the Department of Justice.

Three of the defendants are U.S. citizens, one is from Estonia, three are from Ukraine, two are from the People's Republic of China and one is from Belarus. One individual is only known by an alias online, and his place of origin is unknown.

In an indictment returned on Aug. 5, 2008, by a federal grand jury in Boston, Albert "Segvec" Gonzalez, of Miami, was charged with computer fraud, wire fraud, access device fraud, aggravated identity theft and conspiracy for his role in the scheme. Criminal informations were also released today in Boston on related charges against Christopher Scott and Damon Patrick Toey, both of Miami.

The Boston indictment alleges that during the course of the sophisticated conspiracy, Gonzalez and his co-conspirators obtained the credit and debit card numbers by "wardriving" and hacking into the wireless computer networks of major retailers — including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble, Sports Authority, Forever 21 and DSW. Once inside the networks, they installed "sniffer" programs that would capture card numbers, as well as password and account information, as they moved through the retailers' credit and debit processing networks.

The indictment alleges that after they collected the data, the conspirators concealed the data in encrypted computer servers that they controlled in Eastern Europe and the United

States. They allegedly sold some of the credit and debit card numbers, via the Internet, to other criminals in the United States and Eastern Europe. The stolen numbers were "cashed out" by encoding card numbers on the magnetic strips of blank cards. The defendants then used these cards to withdraw tens of thousands of dollars at a time from ATMs. Gonzalez and others were allegedly able to conceal and launder their fraud proceeds by using anonymous Internet-based currencies both within the United States and abroad, and by channeling funds through bank accounts in Eastern Europe.

Gonzalez was previously arrested by the Secret Service in 2003 for access device fraud. During the course of this investigation, the Secret Service discovered that Gonzalez, who was working as a confidential informant for the agency, was criminally involved in the case. Because of the size and scope of his criminal activity, Gonzalez faces a maximum penalty of life in prison if he is convicted of all the charges alleged in the Boston indictment.

Also today, indictments were unsealed in San Diego against scheme participant Maksym "Maksik" Yastremskiy, of Kharkov, Ukraine, and Aleksandr "Jonny Hell" Suvorov, of Sillamae, Estonia. The indictments charge the defendants with crimes related to the sale of the stolen credit card data that Gonzalez and others illegally obtained, as well as additional stolen credit card data. Suvorov is charged with conspiracy to possess unauthorized access devices, possession of unauthorized access devices, trafficking in unauthorized access devices, identity theft, aggravated identity theft, and aiding and abetting. Yastremskiy is charged with trafficking in unauthorized access devices, identity theft, aggravated identity theft and conspiracy to launder monetary instruments. The indictment also contains a forfeiture allegation.

In addition, an indictment against Hung-Ming Chiu and Zhi Zhi Wang, both of the People’s Republic of China, and a person known only by the online nickname "Delpiero," was also unsealed in San Diego today. Chiu, Wang and Delpiero are charged with conspiracy to possess unauthorized access devices, trafficking in unauthorized access devices, trafficking in counterfeit access devices, possession of unauthorized access devices, aggravated identity theft, and aiding and abetting. Also in San Diego, Sergey Pavolvich, of Belarus, and Dzmitry Burak and Sergey Storchak, both of Ukraine, were charged in a criminal complaint with conspiracy to traffic in unauthorized access devices. All are believed to be foreign nationals residing outside of the United States.

The San Diego charges allege that Yastremskiy, Suvorov, Chiu, Wang, Delpiero, Pavolvich, Burak and Storchak operated an international stolen credit and debit card distribution ring with operations from Ukraine, Belarus, Estonia, the People’s Republic of China, the Philippines and Thailand. The indictments allege that each of the defendants sold stolen credit and debit card information for personal gain. For example, the indictment of Yastremskiy alleges that he received proceeds exceeding $11 million from this criminal activity. These indictments and complaints are the result of a three-year undercover investigation conducted out of the San Diego Field Office of the U.S. Secret Service.

In May 2008, Gonzalez, Suvorov and Yastremskiy also were charged in a related indictment in the Eastern District of New York. The New York charges allege that the trio was engaged in a sophisticated scheme to hack into computer networks run by the Dave & Buster’s restaurant chain, and stole credit and debit card numbers from at least 11 locations. Specifically, the indictment alleges that the defendants gained unauthorized access to the cash register terminals and installed at each restaurant a "packet sniffer," a computer code designed to capture communications on a computer network. The packet sniffer was configured to capture credit and debit card numbers as this information was processed by

the restaurants. At one restaurant location, the packet sniffer captured data for approximately 5,000 credit and debit cards, eventually causing losses of at least $600,000 to the financial institutions that issued the credit and debit cards.

Gonzalez is currently in pre-trial confinement on the New York charges. Based upon the San Diego charges, Turkish officials apprehended Yastremskiy in July 2007 in Turkey when he travelled there on vacation. He has been in confinement since then in Turkey, pending the resolution of related Turkish charges, and the United States has made a formal request for his extradition. At the request of the Department of Justice, Suvorov was apprehended by the German Federal Police in Frankfurt in March 2008 on the San Diego charges when he travelled there on vacation. He is currently in confinement pending the resolution of extradition proceedings.

"So far as we know, this is the single largest and most complex identity theft case ever charged in this country," said Attorney General Mukasey. "It highlights the efforts of the Justice Department to fight this pernicious crime and shows that, with the cooperation of our law enforcement partners around the world, we can identify, charge and apprehend even the most sophisticated international computer hackers."

"While technology has made our lives much easier it has also created new vulnerabilities. This case clearly shows how strokes on a keyboard with a criminal purpose can have costly results. Consumers, companies and governments from around the world must further develop ways to protect our sensitive personal and business information and detect those, whether here or abroad, that conspire to exploit technology for criminal gain," said U.S. Attorney Michael J. Sullivan.

"These prosecutions demonstrate that, through coordinated commitment, the United States Secret Service and the Department of Justice will penetrate and prosecute hacker organizations, wherever based and however sophisticated. The United States Attorney's Office for the Southern District of California is especially gratified that the work of the San Diego field office of the Secret Service contributed to an unprecedented effort to dismantle this international criminal enterprise," said Karen P. Hewitt, U.S. Attorney for the Southern District of California.

"Computer hacking and identity theft pose serious risks to our commercial, personal and financial security," said U.S. Attorney for the Eastern District of New York Benton J. Campbell. "Hackers who reach into our country from abroad will find no refuge from the reach of U.S. criminal justice."

"Technology has forever changed the way commerce is conducted, virtually erasing geographic boundaries," said U.S. Secret Service Director Mark Sullivan. "While these advances and the global nature of cyber crime continue to have a profound impact on our financial crimes investigations, this case demonstrates how combining law enforcement resources throughout the world sends a strong message to criminals that they will be pursued and prosecuted no matter where they reside."

"The Internal Revenue Service Criminal Investigation Division recommends charges in numerous types of financial crimes," said Internal Revenue Service Criminal Investigation (IRS-CI) Chief Eileen Mayer. "Today's indictment is the result of a strong law enforcement partnership that brings together the necessary skills to follow alleged criminal activity from cyberspace to bank accounts. We are committed to the government's efforts to stop this type of corruptive activity."

These cases are being prosecuted by Assistant U.S. Attorney Stephen Heymann of the District of Massachusetts, Assistant U.S. Attorney Orlando Gutierrez of the Southern District of California, Assistant U.S. Attorney Will Campos of the Eastern District of New York, and by Senior Counsel Kimberly Kiefer Peretti, and Trial Attorneys Jenny Ellickson and Evan Williams of the Criminal Division’s Computer Crime & Intellectual Property Section. The Criminal Division's Office of International Affairs provided extensive assistance related to extradition matters. All of theses cases are being investigated by the U.S. Secret Service. The IRS-CI provided significant investigatory assistance in the Boston case.

###

08-689