U.S Department of Homeland Security

United States Secret Service

Press Release

August 5, 2008
Contact: (202) 406-5708
GPA 15-08

ADDITIONAL INDICTMENTS ANNOUNCED IN ONGOING SECRET SERVICE NETWORK INTRUSION INVESTIGATION

(Washington, D.C.) – Indictments were unsealed today in Boston and San Diego against 11 individuals in a U.S. Secret Service investigation into what is believed to be the largest hacking and identity theft case ever prosecuted in the United States. The high-profile cyber investigation by the Secret Service uncovered the theft and sale of more than 40 million credit and debit card numbers from nine major U.S. retailers. The defendants – three are U.S. citizens, one is from Estonia, three are from Ukraine, two are from the People's Republic of China, one is from Belarus and one individual is only known by an online alias – are charged with numerous crimes, including conspiracy, computer intrusion, fraud and identity theft.

"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."

In an indictment returned today, 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. 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.

Criminal informations were also released today in Boston on related charges against Christopher Scott and Damon Patrick Toey, both of Miami. The indictment

-more-

alleges that 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. After they collected the data, the conspirators allegedly 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.

Also today, indictments were unsealed in San Diego against scheme participants 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.

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 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. The 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.

-more-

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.

"These significant arrests are the result of ongoing cooperation among investigators throughout the Secret Service and our domestic and international law enforcement partners," Director Sullivan added. "We continue to effectively address evolving criminal methods and transcend borders by combining our investigative resources."

The United States Secret Service was originally founded in 1865 for the purpose of suppressing the counterfeiting of U. S. currency. Over the years it has grown into one of the premier law enforcement organizations charged with investigating financial crimes. The Secret Service has taken a lead role in the developing area of cyber crime, establishing working partnerships in both the law enforcement and business communities to address such issues as protection of critical infrastructure, Internet intrusions and associated fraud.

# # #

EDITOR'S NOTE: For questions concerning this release, please contact the United States Secret Service Office of Government and Public Affairs at 202-406-5708.