Department of Justice

FOR IMMEDIATE RELEASE
MONDAY, MAY 12, 2008
WWW.USDOJ.GOV

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

HACKERS INDICTED FOR STEALING CREDIT AND DEBIT CARD NUMBERS FROM NATIONAL RESTAURANT CHAIN

WASHINGTON – Three defendants have been charged in a federal grand jury indictment and complaint with illegally accessing the computer systems of a national restaurant chain and stealing credit and debit card numbers from that system, Assistant Attorney General Alice S. Fisher of the Criminal Division and U.S. Attorney for the Eastern District of New York Benton J. Campbell announced today.

The 27-count indictment, returned on March 12, 2008, and unsealed today in Central Islip, N.Y., charges Maksym Yastremskiy, of Kharkov, Ukraine, and Aleksandr Suvorov, of Sillamae, Estonia, with wire fraud conspiracy, wire fraud, conspiracy to possess unauthorized access devices, access device fraud, aggravated identity theft, conspiracy to commit computer fraud, computer fraud and counts of interception of electronic communications. A one-count complaint unsealed today in Central Islip charges Albert Gonzalez of Miami with wire fraud conspiracy related to the scheme.

According to the indictment and complaint, Maksym Yastremskiy, a/k/a "Maksik," Aleksandr Suvorov, a/k/a "JonnyHell," and Albert Gonzales, a/k/a "Segvec," engaged in a scheme in which they hacked into cash register terminals at 11 Dave & Busters, Inc. (D&B) restaurants at various locations around the United States in order to acquire "track 2" credit and debit card information. The defendants then sold the stolen data to others who used it to make fraudulent purchases or re-sold it to make such purchases, causing losses to financial institutions that issued the credit and debit cards. Track 2 data includes the customer's account number and expiration date, but not the cardholder's name or other personally identifiable information.

The indictment alleges that in or about May 2007, Yastremskiy and Suvorov gained unauthorized access to the cash register terminals and installed at each restaurant a "packet sniffer," a malicious piece of computer code designed to capture communications between two or more computer systems on a single network. The packet sniffer was configured to capture track 2 data as it moved from the restaurant's point-of-sale server through the computer system at the company's corporate headquarters to the data processor's computer system. At one restaurant location the packet sniffer captured track 2 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.

Turkish officials arrested Yastremskiy in Turkey in July 2007, and he remains in jail on potential violations of Turkish law. A formal request for extradition of Yastremskiy to the United States has been made to the Turkish government. At the request of the United States, Suvorov was arrested in March 2008 by German officials while he was visiting the country. He remains in jail in Germany, pending German action on a formal U.S. extradition request. U.S. Secret Service officials arrested Gonzalez in Miami in May 2008.

"Operating from locations in the United States and abroad, these defendants hacked into computer systems and stole credit and debit card data from unsuspecting victims for their personal enrichment," said Assistant Attorney General for the Criminal Division Alice S. Fisher. "The Department of Justice will be vigilant against these online hacker schemes that harm the integrity of the marketplace and victimize the public."

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

"This case demonstrates the potential for criminals to inflict significant damage to our nation's financial sector, but this investigation and the resulting indictments should serve as a warning to cyber criminals that law enforcement will continue to pursue them wherever they are," said U.S. Secret Service Director Mark Sullivan. "Cooperation and partnerships have allowed us to focus our resources and respond quickly to uncover and prevent these types of crimes, whether they originate within or outside our borders."

An indictment is a formal accusation of criminal conduct, not evidence. A defendant is presumed innocent unless and until convicted through due process of law.

These cases are being prosecuted by the U.S. Attorney's Office for the Eastern District of New York and the Criminal Division's Computer Crime and Intellectual Property Section. The case is being investigated by the U.S. Secret Service, with full cooperation and assistance from Dave & Buster's. The Criminal Division's Office of International Affairs has provided extensive assistance related to the extradition matters.

###

08-403