Department of Justice

FOR IMMEDIATE RELEASE
Monday, August 17, 2009
WWW.USDOJ.GOV

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

Alleged International Hacker Indicted for Massive Attack on U.S. Retail and Banking Networks

Data Related to More Than 130 Million Credit and Debit Cards Allegedly Stolen

WASHINGTON – Albert Gonzalez, 28, of Miami, Fla., was indicted today for conspiring to hack into computer networks supporting major American retail and financial organizations, and stealing data relating to more than 130 million credit and debit cards, announced Assistant Attorney General of the Criminal Division Lanny A. Breuer, Acting U.S. Attorney for the District of New Jersey Ralph J. Marra Jr. and U.S. Secret Service Assistant Director for Investigations Michael Merritt.

In a two-count indictment alleging conspiracy and conspiracy to engage in wire fraud, Gonzalez, AKA "segvec," "soupnazi" and "j4guar17," is charged, along with two unnamed co-conspirators, with using a sophisticated hacking technique called an "SQL injection attack," which seeks to exploit computer networks by finding a way around the network's firewall to steal credit and debit card information. Among the corporate victims named in the indictment are Heartland Payment Systems, a New Jersey-based card payment processor; 7-Eleven Inc., a Texas-based nationwide convenience store chain; and Hannaford Brothers Co. Inc., a Maine-based supermarket chain.

The indictment, which details the largest alleged credit and debit card data breach ever charged in the United States, alleges that beginning in October 2006, Gonzalez and his co-conspirators researched the credit and debit card systems used by their victims; devised a sophisticated attack to penetrate their networks and steal credit and debit card data; and then sent that data to computer servers they operated in California, Illinois, Latvia, the Netherlands and Ukraine. The indictment also alleges Gonzalez and his co-conspirators also used sophisticated hacker techniques to cover their tracks and to avoid detection by anti-virus software used by their victims.

If convicted, Gonzalez faces up to 20 years in prison on the wire fraud conspiracy charge and an additional five years in prison on the conspiracy charge, as well as a fine of $250,000 for each charge.

Gonzalez is currently in federal custody. In May 2008, the U.S. Attorney's Office for the Eastern District of New York charged Gonzalez for his alleged role in the hacking of a computer network run by a national restaurant chain. Trial on those charges is scheduled to begin in Long Island, N.Y., in September 2009.

In August of 2008, the Justice Department announced an additional series of indictments against Gonzalez and others for a number of retail hacks affecting eight major retailers and involving the theft of

data related to 40 million credit cards. Those charges were filed in the District of Massachusetts. Gonzalez is scheduled for trial on those charges in 2010.

The charges announced today relate to a different pattern of hacking activity that targeted different corporate victims and involved different co-conspirators.

This case is being prosecuted by Assistant U.S. Attorneys Erez Lieberman and Seth Kosto for the U.S. Attorney's Office for the District of New Jersey and by Senior Trial Counsel Kimberly Kiefer Peretti of the Criminal Division's Computer Crime and Intellectual Property Section. The case is being investigated by the U.S. Secret Service.

###

09-810