Department of Justice

FOR IMMEDIATE RELEASE
TUESDAY, DECEMBER 29, 2009
WWW.JUSTICE.GOV

CRM
(202) 514-2008
TDD (202) 514-1888

MAJOR INTERNATIONAL HACKER PLEADS GUILTY FOR MASSIVE ATTACK ON U.S. RETAIL AND BANKING NETWORKS

WASHINGTON- Albert Gonzalez, 28, of Miami, pleaded guilty today to conspiring to hack into computer networks supporting major American retail and financial organizations, and to steal data relating to tens of millions of credit and debit cards, announced Assistant Attorney General of the Criminal Division Lanny A. Breuer, U.S. Attorney for the District of New Jersey Paul J. Fishman, U.S. Attorney for the District of Massachusetts Carmen Milagros Ortiz and Director of the U.S. Secret Service Mark Sullivan.

Gonzalez, aka "segvec," "soupnazi" and "j4guar17," pleaded guilty to two counts of conspiracy to gain unauthorized access to the payment card networks operated by, among others, Heartland Payment Systems, a New Jersey-based card processor; 7-Eleven, a Texas-based nationwide convenience store chain; and Hannaford Brothers Co. Inc., a Maine-based supermarket chain. The plea was entered in federal court in Boston before U.S. District Court Judge Douglas P. Woodlock. The case is one of the largest data breaches ever investigated and prosecuted in the United States.

According to information contained in the plea agreement, Gonzalez leased or otherwise controlled several servers, or "hacking platforms," and gave access to these servers to other hackers, knowing that they would use them to store malicious software, or "malware," and launch attacks against corporate victims. Malware used against several of the corporate victims was also found on a server controlled by Gonzalez. Gonzalez tested malware by running multiple anti-virus programs in an attempt to ascertain if the programs detected the malware. According to information in the plea agreement, it was foreseeable to Gonzalez that his co-conspirators would use malware to steal tens of millions of credit and debit card numbers, affecting more than 250 financial institutions. Gonzalez was indicted in New Jersey in August 2009 for this criminal conduct.

Based on the terms of the plea agreement, Gonzalez will not seek a prison term under 17 years and the government will not seek a prison term of more than 25 years. Gonzalez pleaded guilty in September 2009 in Boston to 19 counts of conspiracy, computer fraud, wire fraud, access device fraud and aggravated identity theft relating to hacks into numerous major U.S. retailers including TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble and Sports Authority. Gonzalez was indicted for those offenses in August 2008 in the District of Massachusetts. Gonzalez also pleaded guilty in September 2009 in Boston to one count of conspiracy to commit wire fraud relating to hacks into the Dave & Buster's restaurant chain, which were the subject of a May 2008 indictment in the Eastern District of New York.

As part of the plea agreement with the government, the New Jersey case was transferred to the District of Massachusetts for plea and sentencing. According to the terms of the New Jersey plea agreement, the parties agree that Gonzalez' sentence in the New Jersey case should run concurrently

with the sentence imposed in the Boston and New York cases. Gonzalez remains in federal custody. Sentencing in the Boston and New York cases is currently scheduled for March 18, 2010, in Boston. Sentencing in the New Jersey case is scheduled for March 19, 2010.

"The Department of Justice will not allow computer hackers to rob consumers of their privacy and erode the public's confidence in the security of the marketplace," said Assistant Attorney General Breuer. "Criminals like Albert Gonzalez who operate in the shadows will be caught, exposed and held to account. Indeed, with timely reporting of data breaches and high-tech investigations, even the most sophisticated hacking rings can be uncovered and dismantled, as our prosecutors and agents demonstrated in this case."

"Commercial hackers like Gonzalez believe they are immune from detection and prosecution as they lurk in the shadows of the Internet," said U.S. Attorney Fishman of the District of New Jersey. "But time and again they are caught, prosecuted and sentenced to lengthy federal prison terms. Other hackers should sit up and take notice."

"The conviction of Mr. Gonzalez, and the unraveling of one of the most complex and large scale identity theft cases in history, should serve as a reminder to hacker organizations, that the Department of Justice will vigorously investigate and prosecute cybercrimes, regardless of their sophistication and global reach. Mr. Gonzalez's conviction is the result of unprecedented coordination across agency and geographical lines, and I want to commend the investigators and prosecutors who have worked tirelessly to bring this case to fruition," said U.S. Attorney Ortiz of the District of Massachusetts.

"Today's plea proves that although cyber criminals can threaten our nation's financial sector, the Secret Service and its many partners around the world will pursue and prosecute them," said U.S. Secret Service Director Sullivan. "Time and again, cooperation and advanced methodologies have allowed us to focus our resources in order to detect and prevent these types of crimes, wherever they originate."

The New Jersey case is being prosecuted by Assistant U.S. Attorneys Erez Liebermann and Seth Kosto of the District of New Jersey, Assistant U.S. Attorneys Stephen Heymann and Donald Cabell of the District of Massachusetts, and Senior Counsel Kimberly Kiefer Peretti of the Criminal Division's Computer Crime and Intellectual Property Section. All of these cases are being investigated by the U.S. Secret Service.

###

09-1389