Department of Justice

FOR IMMEDIATE RELEASE CRM

FRIDAY, MARCH 26, 2010 (202) 514-2008

WWW.JUSTICE.GOV TDD (202) 514-1888

LEADER OF HACKING RING SENTENCED FOR MASSIVE IDENTITY THEFTS FROM PAYMENT PROCESSOR AND U.S. RETAIL NETWORKS

WASHINGTON – The leader of the largest hacking and identity theft ring ever prosecuted by the U.S. government has been sentenced to 20 years and one day in prison for his role in a series of hacks into a major payment processor and several retail networks, announced Assistant Attorney General for the Criminal Division Lanny A. Breuer; U.S. Attorney for the District of Massachusetts Carmen Milagros Ortiz; U.S. Attorney for the Eastern District of New York Benton J. Campbell; U.S. Attorney for the District of New Jersey Paul J. Fishman; and Director of the U.S. Secret Service Mark Sullivan.

On March 25, 2010, Albert Gonzalez, 28, of Miami, was sentenced by U.S. District Court Judge Patti B. Saris in U.S. District Court in Boston to 20 years in prison for conspiracy, computer fraud wire fraud, access device fraud and aggravated identity theft related to hacks into numerous major U.S. retailers, including the TJX Companies, BJ's Wholesale Club, OfficeMax, Boston Market, Barnes & Noble and Sports Authority.

Thursday's sentence also addresses the charges brought in the Eastern District of New York and transferred to Boston for plea and sentence. The New York indictment charged Gonzalez with, among other things, conspiracy to commit wire fraud relating to his breach of the electronic payment systems of the Dave and Buster's restaurant chain. Gonzalez was also ordered to serve three years of supervised release following his prison term and to pay a fine of $25,000.

Today, Gonzalez was sentenced by U.S. District Court Judge Douglas P. Woodlock to 20 years and one day in prison for two counts of conspiracy relating to his efforts to assist others in gaining access to the payment card networks of 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. Gonzalez was also ordered to serve three years of supervised release following his prison term. The prison term and the term of supervised release will run concurrently with the sentence imposed yesterday against Gonzalez. Gonzalez was ordered to pay a fine of $25,000 in addition to the fine imposed yesterday. The charges in this case were originally brought in the District of New Jersey. Restitution in all three cases will be determined by the court at a later date.

“Every day, as cyber criminals try to steal the debit and credit card numbers of unsuspecting American consumers, federal agents and prosecutors are there to catch them,” said Assistant Attorney General Lanny A. Breuer. “These sentences – some of the longest ever imposed for hacking crimes – send a powerful message to hackers around the globe that U.S. law enforcement will not allow them to breach American computer networks and payment systems, or illegally obtain identities.”

“Investigations of this magnitude – the largest of its kind in the country - remind us that as technology rapidly advances, so do our vulnerabilities. While electronic payments are simply a way of life, we must be mindful that with the stroke of the keyboard, criminal enterprises can strike from anywhere in the world,” said U.S. Attorney Carmen M. Ortiz. “I want to assure consumers that we continue to use all available resources to detect and investigate computer hacking crimes, no matter where in the world they are committed.”

“Computer hackers and identity thieves pose serious risks to our commercial, personal and financial security,” stated U.S. Attorney for the Eastern District of New York Benton J. Campbell. “Today’s sentence should serve as a warning to would-be hackers everywhere, including those who commit their crimes from abroad – you will be found, prosecuted and convicted.”

“These sentences reflect the tremendous harm Mr. Gonzalez caused millions of innocent Americans,” said U.S. Attorney Paul J. Fishman of the District of New Jersey. “They go a long way to deterring like-minded criminals who mistakenly believe they can escape arrest and prosecution by committing their crimes online and hiding behind a computer screen. This investigation demonstrates the ongoing commitment of the Department of Justice to ensure the safety and security of online commercial transactions.”

“Technology has virtually erased geographic boundaries and changed the way we do business,” said U.S. Secret Service Director Mark Sullivan. “As we have seen with this case, even with the increasing complexity of network intrusions, it remains difficult for criminals to remain anonymous. The Secret Service continues to seek new and innovative ways to combat emerging cyber threats. Our success in this case and similar investigations is a result of our close work with our worldwide network of law enforcement partners.”

According to court documents related to his conviction in the Massachusetts and New York cases, Gonzalez and his co-conspirators broke into retail credit card payment systems through a series of sophisticated techniques, including “wardriving” and installation of sniffer programs to capture credit and debit card numbers used at the victim retail stores. Wardriving involves driving around in a car with a laptop computer looking for unsecure wireless computer networks of retailers. Using these techniques, Gonzalez and his co-defendants were able to steal more than 40 million credit and debit card numbers from victim retailers. According to court documents, Gonzalez and his co-conspirators sold the numbers to others for their fraudulent use and engaged in ATM fraud by encoding the data on the magnetic stripe of blank cards and withdrawing thousands of dollars at a time from ATMs.

Gonzalez and his co-conspirators concealed and laundered 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's co-conspirators were located throughout the United States, Estonia and the Ukraine. In the New Jersey case, Gonzalez provided malware to other hackers that allowed them to circumvent anti-virus programs and firewalls, and gain access to the victim companies' networks. Gonzalez admitted in court documents that it was foreseeable that, based upon his assistance, his co-conspirators would be able to steal tens of millions of credit and debit card numbers, affecting more than 250 financial institutions.

To date, six co-conspirators have pleaded guilty in the United States. One co-conspirator, an Estonian national, was apprehended at the United States' request by German authorities while he was travelling in Germany. He was subsequently extradited to the United States, where he pleaded guilty to his role in the hacking and identity theft scheme. Another co-conspirator was arrested and convicted in Turkey on related identity theft charges, and was sentenced to 30 years in prison.

The Boston case was prosecuted by Assistant U.S. Attorneys Stephen Heymann and Donald Cabell of the District of Massachusetts. The New York case was prosecuted by Assistant U.S. Attorney William Campos of the Eastern District of New York and by Senior Counsel Kimberly Kiefer Peretti and Trial Counsel Evan Williams of the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS). The New Jersey case was prosecuted by Assistant U.S. Attorneys Erez Liebermann and Seth Kosto for the District of New Jersey, Assistant U.S. Attorney Stephen Heymann for the District of Massachusetts and by Senior Counsel Kimberly Kiefer Peretti of CCIPS. All of these cases were investigated by the U.S. Secret Service.

###

10-329