Department of Justice

FOR IMMEDIATE RELEASE
FRIDAY, APRIL 11, 2008
WWW.USDOJ.GOV

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

Foreign National Sentenced to Nine Years in Prison for Hotel Business Center Computer Fraud Scheme

WASHINGTON - Mario Simbaqueba Bonilla, 40, a Colombian citizen, was sentenced today to nine years in prison, resulting from his guilty plea to a 16-count indictment involving a complex computer fraud scheme victimizing more than 600 people, Assistant Attorney General Alice S. Fisher of the Criminal Division, U.S. Attorney Alex Acosta for the Southern District of Florida, the U.S. Department of Defense, Defense Criminal Investigative Service (DCIS), and the U.S. Postal Inspection Service announced today. Simbaqueba Bonilla was also sentenced to three years supervised release upon his release from prison and ordered to pay restitution of $347,000.

On Jan. 9, 2008, Simbaqueba Bonilla pleaded guilty to charges of conspiracy, access device fraud and aggravated identity theft. According to the charges and in-court statements Simbaqueba Bonilla, alone and in concert with a co-conspirator, engaged in a complex series of computer intrusions, identity thefts, and credit card frauds designed to steal money from payroll, bank and other accounts of their victims. The Court recognized the attempted and actual loss from the scheme at $1.4 million. Much of the identity theft activity – initiated by Simbaqueba Bonilla from computers in Colombia – targeted individuals residing in the United States, including Department of Defense personnel. Simbaqueba Bonilla used the money to buy expensive electronics and luxury travel and accommodations in various countries, including Hong Kong, Turks and Caicos, France, Jamaica, Italy, Chile and the United States.

Simbaqueba Bonilla, as outlined in the indictment and information offered at his plea hearing, engaged in a conspiracy from approximately 2004 to 2007 that began with illegally installing keystroke logging software on computers located in hotel business centers and Internet lounges around the world. This software would collect the personal information of those who used the computers, including passwords and other personal identifying information the victims used to access their bank, payroll, brokerage and other accounts online. Simbaqueba Bonilla used the

data he intercepted from his victims, who were typically guests at hotels throughout the country, to steal or divert money from their accounts into other accounts he had created in the names of other people he had victimized in the same way. Then, through a complex series of electronic transactions designed to cover his trail, Simbaqueba Bonilla would transfer the stolen money to credit, cash or debit cards and have the cards mailed to himself and others at commercial mailing addresses he opened across the country.

Federal agents arrested Simbaqueba Bonilla when he flew into the United States in August 2007. At the time of his arrest, Simbaqueba Bonilla was flying on an airline ticket purchased with stolen funds, and had in his possession a laptop also purchased with stolen funds. That laptop contained the names, passwords, and other personal and financial information of more than 600 people.

The case was prosecuted jointly by Trial Attorney William Yurek of the Criminal Division's Computer Crime and Intellectual Property Section and Assistant U.S. Attorney Richard Domingues Boscovich of the U.S. Attorney's Office in Miami, who serves as the coordinator for the office's Computer Hacking and Intellectual Property Unit. The criminal investigation was conducted by agents of the U.S. Department of Defense, Defense Criminal Investigative Service and the U.S. Postal Inspection Service.

###

08-294