The United States Attorney's Office

Southern District of Florida

Press Release

FOREIGN NATIONAL PLEADS GUILTY IN COMPLEX COMPUTER FRAUD SCHEME VICTIMIZING HUNDREDS OF INDIVIDUALS

January 9, 2008

FOR IMMEDIATE RELEASE

A Colombian citizen pled guilty today to a 16-count indictment involving a complex computer fraud scheme victimizing over 600 people, Assistant Attorney General Alice S. Fisher of the Criminal Division and U.S. Attorney Alex Acosta for the Southern District of Florida and U.S. Department of Defense, Defense Criminal Investigative Service and the United States Postal Inspection Service announced today.

According to the indictment, **Mario Simbaqueba Bonilla**, 40, alone and in concert with a co-conspirator, engaged in a complex series of computer intrusions, aggravated identity thefts and credit card frauds designed to steal money from payroll, bank and other accounts of their victims. Much of the identity theft activity – initiated by Simbaqueba Bonilla from computers in Colombia – targeted individuals residing in the U.S., 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.

“Today's plea sends a message to identity thieves everywhere who believe the Internet provides them with anonymity that cloaks their detection from justice," said Assistant Attorney General Alice S. Fisher of the Criminal Division. "The Department of Justice remains committed to prosecuting even the most sophisticated cases involving cyber crimes, identity theft, and other crimes that victimize our citizens and plague our economy."

R. Alexander Acosta, U.S. Attorney for the SDFL, stated, “Unfortunately, this is not an isolated case. The Internet is an outstanding tool, but it is vulnerable. Criminals like Bonilla use the Internet to steal our banking and personal data, and then our money. When you travel, please think twice before entering personal or financial data on a public computer.”

Richard D. Zott, Special Agent in Charge, DCIS, stated, “Investigating computer crimes that affect the integrity and security of the Department of Defense and its personnel is a priority for the Defense Criminal Investigative Service (DCIS). This case demonstrates that DCIS will expend the needed resources to investigate these types of allegations, regardless of where the subject is located.”

“This case demonstrates that law enforcement's commitment to pursuing even the most sophisticated criminal schemes thwarts the thieves' abilities to execute them. Although technology has made crime global, the Postal Inspection Service will not be limited by border constraints,” said Henry Gutierrez, Inspector in Charge, U.S. Postal Inspection Service, Miami Division.

Simbaqueba Bonilla, as outlined in the indictment and the proffer of facts offered at his guilty plea hearing, engaged in a conspiracy 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 Pak Mail and other commercial mailing addresses he opened across the country.

Federal agents arrested Simbaqueba Bonilla when he flew into the United States last August. 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 Senior Counsel William Yurek of the Computer Crime and Intellectual Section of the Criminal Division 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 (CHIP). The criminal investigation was conducted by agents of the U.S. Department of Defense, Defense Criminal Investigative Service and the United States Postal Inspection Service.

Attachments:
Indictment (PDF)

A copy of this press release may be found on the website of the United States Attorney's Office for the Southern District of Florida at http://www.usdoj.gov/usao/fls. Related court documents and information may be found on the website of the District Court for the Southern District of Florida at http://www.flsd.uscourts.gov or on http://pacer.flsd.uscourts.gov.

Technical comments about this website can be e-mailed to the Webmaster. PLEASE NOTE: The United States Attorney's Office does not respond to non-technical inquiries made to this website. If you wish to make a request for information, you may contact our office at 305-961-9001, or you may send a written inquiry to the United States Attorney's Office, Southern District of Florida, 99 NE 4th Street, Miami, Fl. 33132.