NEWS

United States Department of Justice
U.S. Attorney, District of New Jersey
970 Broad Street, Seventh Floor
Newark, New Jersey 07102

Ralph J. Marra, Jr., Acting U.S. Attorney

More Information? Call the Assistant U.S. Attorney or other contact listed below to see if more information is available.

News on the Internet: News Releases and related documents are posted at our website, along with links to our archived releases for other years. ***Go to: www.usdoj.gov/usao/nj/publicaffairs***

Contact:
Michael Drewniak, PIO
973-645-2888

pena0217.rel
FOR IMMEDIATE RELEASE
Feb. 17, 2009

Computer Hacker Fugitive Apprehended and Indicted for Fraud that Victimized Phone Service Providers

(More)

NEWARK, N.J. – A Miami man charged in 2006 with secretly hacking into the computer networks of unsuspecting Internet phone service providers was indicted today by a federal grand jury, Acting U.S. Attorney Ralph J. Marra announced.

The indictment of Edwin Andres Pena follows his apprehension on Feb. 6 in Mexico, where he now is in custody and awaits extradition. Pena has been a fugitive since posting bond and fleeing prosecution after his arrest in June 2006 in Miami.

Pena, 26, was indicted on fraud and computer hacking charges for his role in a scheme to defraud Voice Over Internet Protocol (VoIP) telephone service providers. Pena, who purported to be a legitimate wholesaler of these Internet-based phone services, allegedly sold discounted service plans to his unsuspecting customers. The Indictment alleges that Pena was able to offer such low prices because he would secretly hack into the computer networks of unsuspecting VoIP providers, including one Newark-based company, to route his customers' calls.

Through this scheme, Pena is alleged to have sold more than 10 million minutes of Internet phone service to telecom businesses at deeply discounted rates, causing a loss of more than $1.4 million in less than a year. The victimized Newark-based company, which transmits VoIP services for other telecom businesses, was billed for more than 500,000 unauthorized telephone calls routed through its calling network that were "sold" to the defendant's unwitting customers at those deeply discounted rates, according to the Indictment.

Pena, 26, a permanent legal resident of the United States of Venezuelan origin, allegedly enlisted the help of others, including a professional "hacker" in Spokane, Washington. The hacker, named in the Indictment as Robert Moore, 24, pleaded guilty in the District of New Jersey on March 7, 2007, to federal hacking charges for assisting Pena in this scheme. Moore was sentenced to 24 months in prison on March 8, 2008, and is currently incarcerated. Moore admitted at his plea hearing to conspiring with Pena and to performing an exhaustive scan of computer networks of unsuspecting companies and other entities in the United States and around the world, searching for vulnerable ports to infiltrate their computer networks to use them to route calls.

Pena was first charged on June 6, 2006, in the District of New Jersey in a criminal Complaint that set forth the scheme described in today's indictment. He was arrested on that Complaint on June 7, 2006, and released the next day on $100,000 bail set by a federal magistrate judge in Florida. Pena appeared in Court in New Jersey on June 29, 2006, and on approximately Aug. 12, 2006, Pena allegedly fled the country to avoid prosecution. He was apprehended by Mexican authorities on Feb 6, 2009, and is currently being held in Mexico on the District of New Jersey's charges. The United

States intends to seek extradition.

The underlying Complaint against Pena sets forth that, to disguise the money obtained from the hacking scheme, Pena purchased real estate, new cars, and a 40-foot motor boat, and put all of that property except for one car in the name of another individual identified in the Complaint as "A.G." Following his June 2006 arrest, federal agents executed a seizure warrant for Pena's 2004 BMW M3, which was purchased and significantly customized with proceeds from Pena's scheme.

The 20-Count Indictment charges wire fraud, computer hacking and conspiracy, and covers conduct occurring between about November 2004 and about May 2006. Rather than purchase VoIP telephone routes for resale, Pena – unbeknownst to his customers – created what amounted to "free" routes by surreptitiously hacking into the computer networks of unwitting, legitimate VoIP telephone service providers and routing his customers' calls in such a way as to avoid detection.

To avoid detection when establishing the "free" calling routes, Pena allegedly recruited Moore, who, through hacking techniques, performed an exhaustive scan of computer networks of unsuspecting companies and other entities in the U.S. and around the globe, searching for vulnerable ports to infiltrate their computer networks. According to records obtained from AT&T, between about June 2005 and about October 2005, for example, more than 6 million scans were initiated by Moore in search of vulnerable network ports. During the same period, AT&T records reveal only two other users with a greater number of scans on its entire global network.

After receiving information from Moore, Pena allegedly reprogrammed the vulnerable computer networks to accept VoIP telephone call traffic. He then routed the VoIP calls of his customers over those networks. In this way, Pena made it appear to the VoIP telephone service providers that the calls were coming from a third party's network.

By sending calls to the VoIP telephone service providers through the unsuspecting third party's networks, the VoIP telephone service providers were unable to identify the true sender of the calls for billing purposes. Consequently, individual VoIP Telecom Providers incurred aggregate routing costs of up to approximately $300,000 per provider, without being able to identify and bill Pena.

An Indictment is merely an accusation, and all defendants are presumed innocent unless and until proven guilty beyond a reasonable doubt.

Wire fraud carries a maximum penalty of 20 years in prison and a $250,000 fine. Conspiracy and the computer hacking violation – fraud and related activity in connection

with computers – each carries a maximum penalty of five years in prison and a fine of $250,000.

Marra credited the Special Agents of the FBI, under the direction of Special Agent in Charge Weysan Dun in Newark, with the investigation.

The case is being prosecuted by Assistant U.S. Attorney Erez Liebermann in the U.S. Attorney's Office Computer Hacking and Intellectual Property group, within the Commercial Crimes Unit.

-end-