July 21, 2004

Department of Justice
CRM
(202) 514-2007
TDD (202) 514-1888
WWW.USDOJ.GOV

Florida Man Charged With Breaking Into Acxiom Computer Records Intrusion and Theft of Data Result in Loss of More than $7 Million

WASHINGTON, D.C. -- Christopher A. Wray, Assistant Attorney General of the Justice Department's Criminal Division, and Bud Cummins, United States Attorney of the Eastern District of Arkansas, announced today that Scott Levine, who effectively controlled Snipermail.com, Inc., has been indicted by a federal grand jury for conspiracy, unauthorized access of a protected computer, access device fraud, money laundering and obstruction of justice. The charges stem from an alleged scheme to steal vast amounts of personal information from a company database and represent what may be the largest cases of intrusion of personal data to date. Levine, 45, of Boca Raton, Florida, was charged in a 144 count indictment filed today in the U.S. District Court in Little Rock. Snipermail, a Florida corporation located in the Boca Raton area, was engaged in the business of distributing advertisements via the Internet to e-mail addresses on behalf of advertisers or their brokers. The charges stem from alleged illegal intrusions by Levine and other Snipermail employees into a computer database owned and operated by Acxiom Corporation, one of the world's largest companies that manages personal, financial, and corporate data. Acxiom, which is headquartered in Little Rock and Conway, Arkansas, stores and processes large amounts of customer-provided data on behalf of its clients. The indictment charges 139 counts of illegal access, representing approximately 8.2 gigabytes of data which were downloaded from the Acxiom server from approximately April 2002 to August 2003. "The protection of personal information stored on our nation's computer systems is critical to public trust in those networks and to the health of our economy," said Assistant Attorney General Christopher Wray. "We will aggressively pursue those who steal private information from computer networks and make it clear that there are serious consequences for such behavior." In July 2003, investigators with the Sheriff's Office in Hamilton County, Ohio, discovered during the course of an unrelated investigation that an Ohio resident named Daniel Baas had illegally entered into an Acxiom file transfer protocol (ftp) server and had downloaded significant amounts of data. Baas subsequently pleaded guilty to federal charges in Ohio on December 2, 2003. During the course of that investigation, and in follow up internal investigations conducted by Acxiom, investigators discovered a second set of intrusions into Acxiom. Those intrusions came from a different internet protocol address and form the basis of the indictment of Scott Levine. Upon discovery of the second set of intrusions, Acxiom immediately sought assistance from the U.S. Attorney's Office for the Eastern District of Arkansas, the Federal Bureau of Investigation (FBI) and the United States Secret Service (USSS). Those agencies formed a task force which utilized the efforts of personnel at the FBI's Regional Computer Forensics Laboratory in Dallas, Texas, along with teams of computer forensic experts from the FBI and USSS. The indictment alleges that these investigators traced the apparent source of the downloads to Snipermail's computer systems. Further investigation

revealed that beginning in April 2002, individuals employed at Snipermail allegedly obtained access to databases on the ftp.acxiom.com server in Conway, Arkansas, and by the spring of 2003, started regularly accessing large data files from that server and downloading them. This activity continued through July 2003, the indictment alleges. In addition, the indictment alleges that Levine and others actively concealed computers from investigators during the course of the investigation in order to hide their illicit activity and avoid prosecution. The victim corporation in this case, Acxiom, immediately notified law enforcement upon discovery of intrusions into its system and has provided exemplary cooperation throughout this investigation. Its quick response and sustained efforts to facilitate this investigation minimized the possible damage and maximized the ability of law enforcement to insure that justice be done.

While the stolen data contained personal information about a great number of individuals and could have resulted in tremendous loss if the information were used in a fraudulent scheme, there is no evidence to date that any of the data was misused in this way. Six other individuals associated with Sniper mail have agreed to cooperate in this investigation.

Members of the public are reminded that the indictment contains only charges. A defendant is presumed innocent of the charges, and it will be the government's burden to prove a defendant's guilt beyond a reasonable doubt at trial. 04-501

###