March 13, 2003

U.S. Department of Justice
United States Attorney
Eastern District of California
501 I Street, Suite 10-100
Sacramento, California 95814
Phone: (916) 554-2700
Fax: (916) 554-2900

Computer Hacker Pleads Guilty To Computer Intrusion and Credit Card Fraud

Defendant admits defacing Air Force Base web site, hacking into three other sites and obtaining and using stolen credit card information.

SACRAMENTO - United States Attorney John K. Vincent announced today that ADIL YAHYA ZAKARIA SHAKOUR, 18, of Los Angeles, California, pled guilty to committing fraud and related activity in connection with computers, and credit card fraud, in violation of 18 U.S.C. §§ 1030(a)(4), 1029(a)(2). According to court documents, during an ongoing investigation, investigators with the Sacramento Valley Hi-Tech Crimes Task Force and the FBI Sacramento Office determined that defendant Shakour committed a series of unauthorized computer intrusions into four separate computer systems inside and outside of California. Additionally, defendant Shakour obtained credit card and personal information from one of the unauthorized computer intrusions and used the information to commit credit card fraud concerning individuals from around the country. After pursuing investigative leads, on October 8, 2002 a federal search warrant was executed at defendant Shakour's Los Angeles residence which confirmed the unauthorized intrusions and credit card fraud along with other evidence. Computer Intrusion at Pro Systems, Inc. and Credit Card Fraud According to the plea agreement, between August 2001 and May 10, 2002, and also on June 22, 2002, and September 10, 2002, defendant Shakour hacked into a computer of Cheaptaxforms.com, located in Mathews, North Carolina, which is a subsidiary of Pro Systems, Incorporated. Defendant Shakour gained unauthorized access with the intent to obtain the credit card and personal information from the Cheaptaxforms.com website, which he then used to purchase items for his personal use. The credit card victims were located around the country, including in Austin, Texas; Granada Hills, California; Colchester, Connecticut; Rockford, Illinois; Lenexa, Kansas; and Rockhill, South Carolina. The fraudulent credit card purchases totaled approximately $7,167. Some of the items purchased included a ring valued at approximately $2,000; a bracelet worth about $1,500; and a necklace worth approximately $500; six two-way pagers; a Sony Playstation 2; and miscellaneous computer parts (including ten Network Interface Cards and two routers). Law enforcement officials contacted each victim who indicated the charges were not authorized. Other Computer Intrusions at Eglin Air Force Base in Florida, Accenture in Chicago, Illinois, and Sandia National Laboratories in Livermore, California

According to court documents, on April 26 and 27, 2002, and May 3 and 6, 2002, defendant Shakour made a series of unauthorized computer intrusions into a server at Eglin Air Force Base, a federal military base in Florida. The objective of the intrusion was to compromise the integrity

of the system, obtain root-level administrator access to the system, and to deface the web site. Shortly after the intrusion, the Web page hosted by the computer was defaced. The text of the defacement denounced the Israeli advancement into Palestine and gave credit to "Anti India Crew" (AIC) for the defacement. The defendant's defacement of the web site and unauthorized access resulted in losses preliminarily estimated to be approximately $75,000. On May 5, 2002, defendant Shakour made an unauthorized computer intrusion from California into the computers of Accenture, a management consulting and technology services company, based in Chicago, Illinois. The defendant's unauthorized access, which compromised the system, resulted in losses preliminarily estimated to be approximately $15,200. On May 6, 2002, defendant Shakour made an unauthorized computer intrusion from California into an unclassified network computer at the Sandia National Laboratories in Livermore, California. The defendant's unauthorized access, which compromised the system, resulted in losses preliminarily estimated to be approximately $2,732.36. According to Assistant U.S. Attorney Mark L. Krotoski, who is prosecuting the case, defendant SHAKOUR faces a maximum penalty of five years and a fine of up to $250,000 for committing fraud and related activity in connection with computers. On the credit card fraud charge, the maximum sentence is ten years and a fine of $250,000. Krotoski added that in the plea agreement, the defendant agreed to make total restitution for his conduct, which is estimated to be approximately $100,000, and will be determined during the sentencing process. The sentencing hearing for SHAKOUR is set for June 12, 2003 before U.S. District Court Judge David F. Levi. The case was investigated by the Sacramento Valley Hi-Tech Crimes Task Force, and Federal Bureau of Investigation Sacramento Office with the assistance of the Los Angeles County District Attorney's Office and the U.S. Attorney's Office for the Central District of California.

###