Department of Justice

FOR IMMEDIATE RELEASE **CRM**
THURSDAY, NOVEMBER 20, 2003 **(202) 514-2007**
WWW.USDOJ.GOV **TDD (202) 514-1888**

JUSTICE DEPARTMENT ANNOUNCES 'OPERATION CYBER SWEEP' TARGETING ONLINE ECONOMIC FRAUD

WASHINGTON, D.C. – Attorney General John Ashcroft, Assistant Attorney General Christopher A. Wray of the Criminal Division, FBI Assistant Director Jana Monroe and Federal Trade Commission Chairman Tim Muris today announced the arrests or convictions of more than 125 individuals and the return of over 70 indictments in a coordinated nationwide enforcement operation designed to crack down on the leading types of online economic crime.

The ongoing operation, known as Operation Cyber Sweep, was coordinated by 34 U.S. Attorneys' offices nationwide, the FBI, the Postal Inspection Service, the FTC, the United States Secret Service, and the Bureau of Immigration and Customs Enforcement, together with a variety of state, local and foreign law enforcement agencies.

The operation targets a variety of online economic crimes that involved schemes including fraud, software piracy and the fencing of stolen goods. The investigation exposes the ways in which economic crimes are becoming increasingly global and multijurisdictional in nature.

"Online criminals assume that they can conduct their schemes with impunity," said Attorney General John Ashcroft. "Operation Cyber Sweep is proving them wrong, by piercing the criminals' cloak of anonymity and prosecuting them to the fullest extent of the law."

More than 125 investigations have been opened since Operation Cyber Sweep began on Oct. 1, 2003. Investigators have uncovered more than 125,000 victims with estimated losses of more than $100 million. More than 90 search and seizure warrants were executed as part of the operation, and prosecutors have obtained more than 70 indictments to date. The charges have led to more than 125 arrests or convictions.

Some of the charges filed in districts throughout the country include:

- In the Central District of California and in Connecticut, Albert Mayzels pleaded guilty to charges in two separate indictments for unauthorized use of access devices and conspiracy to possess counterfeit checks as part of an Internet fraud scheme against online retailer Outpost.com. Specifically, Mayzels admitted to obtaining stolen credit card numbers from various individuals to purchase more than $80,000 in computer equipment and electronic devised from Kent, Connecticut-based Outpost.com.

- In the Eastern District of Virginia and the Eastern District of Tennessee, 21-year-old K.C. Smith pleaded guilty to two felony charges of securities fraud. Smith admitted to using the Internet in 2002 to promote a fraudulent scheme that promised investors high returns on their "international tax-free" investments in the "Maryland Investment Club," a fictitious enterprise. After moving to Tennessee, Smith continued advertising his bogus enterprise through the use of unsolicited bulk e-mail, commonly referred to as spam. Smith was sentenced to 14 months in prison.

- In the Eastern District of Pennsylvania, Allan E. Carlson was indicted on charges of hacking into computers of unsuspecting users across the country to launch spam e-mail attacks criticizing the Philadelphia Phillies baseball team. Carlson, a disgruntled Phillies fan, was also charged with identity theft for illegally using the e-mail address of reporters at Philadelphia newspapers.

- In the Eastern District of Virginia, Helen Carr pleaded guilty to conspiracy to possess unauthorized access devices. The defendant engaged in "phishing" by sending fake e-mail messages to America Online customers, advising that they must update their credit card/personal information on file with AOL to maintain their accounts.

"Cyber crime will continue to be one of the FBI's highest priorities for the foreseeable future," stated FBI Assistant Director Jana Munroe. "The results of Operation Cyber Sweep should send a clear warning to those criminals who exploit technology and use the Internet to commit criminal acts. The FBI, in conjunction with our law enforcement and private sector partners, will move swiftly and aggressively to pursue these criminals world-wide."

"By coordinating our law enforcement efforts with other federal, state and local law enforcers, we leverage our efforts and maximize our impact," said Timothy J. Muris, chairman of the Federal Trade Commission. "We intend to send a strong message to those who use the Internet to break the law: Cyberspace is not outer space and we will trace you, track you and stop you."

Chief Postal Inspector Lee R. Heath added, "Operation Cyber Sweep illustrates how criminals, using today's technological tools and the Internet, still rely on the traditional backbone of commerce—the U. S. Mail—to try to defraud the American public."

Secret Service Director W. Ralph Basham stated: "The success of the United States Secret Service's Electronic Crimes Task Force initiative is a good example of how working partnerships between law enforcement and the private sector are closing the door on criminal intent on exploiting the Internet. These task forces are speeding the process by which different criminal schemes are identified and prosecuted by law enforcement, preventing some of these

crimes from happening, and leading the way to quicker prosecutions, both domestically and internationally."

Operation Cyber Sweep was launched in response to an increase in the reporting of Internet-related complaints to federal agencies. The Internet Fraud Complaint Center (IFCC) – a joint project of the FBI and the National White-Collar Crime Center – reported that in the first nine months of 2003, it referred 58,392 Internet-related fraud complaints to law enforcement. In contrast, in all of calendar year 2002, the IFCC referred about 48,000 Internet-related fraud complaints to law enforcement. The FTC reported that more than one-third of the 218,000 fraud complaints it received in 2002 were Internet-related fraud complaints.

Operation Cyber Sweep is a follow-up to Operation E-Con, which was announced by Attorney General Ashcroft in May 2003. E-Con resulted in the execution of 70 search and seizure warrants and charges against more than 130 individuals.

Victims of online crime are encouraged to file a complaint online with the Internet Fraud Complaint Center, or IFCC. The IFCC is a joint venture of the FBI and the National White Collar Crime Center. The IFCC staff reviews complaints, looking for patterns or other indicators of significant criminal activity, and refers investigative packages of complaints to the appropriate law enforcement authorities in a particular city or region. Victims can find the online form at www.ifccfbi.gov. (The Federal Trade Commission also has an online form for complaints about consumer fraud and deception, available through its website, www.ftc.gov.)

For more information on this initiative and other fraud related matters, please visit the Department's website at www.usdoj.gov.

###

03-638