Department of Justice

FOR IMMEDIATE RELEASE
TUESDAY, AUGUST 5, 2008
WWW.USDOJ.GOV

OPA
(202) 514-2007
TDD (202) 514-1888

FACT SHEET: DEPARTMENT OF JUSTICE EFFORTS TO COMBAT CYBER CRIMES

In May 2006, President Bush created an interagency Identity Theft Task Force, chaired by the Attorney General and co-chaired by the Federal Trade Commission (FTC) Chairman. After examining government and private sector efforts in the identity theft area, the Task Force in April 2007 issued a report to the President with 31 recommendations to improve our national efforts to combat identity theft. These recommendations included protecting personal data in the private and public sector, investigating and prosecuting data breaches and related identity theft, and assisting victims of identity theft. Since then, the Task Force has worked to implement these 31 recommendations over the last year across the government and with our private sector and international partners.

The Department of Justice has supported this Task Force through the vigorous prosecution of the various forms of identity theft. The Department's identity theft prosecutions have ranged from simple theft of financial data and documents to credit-card "skimming" operations; high-tech "phishing" schemes; and schemes to use others' online brokerage accounts to manipulate securities markets.

- **Identity Theft Prosecutions** – As just one example of the Department's robust efforts to prosecute identity thieves, the Department has made extensive use of the aggravated identity theft statute since it was enacted in 2004. During fiscal year 2007, 2,470 defendants were charged federally with identity theft under either 18 U.S.C. §§ 1028 or 1028A. During the same year, 1,943 convictions were obtained under those statutes, and 95.39 percent of the cases resolved resulted in a conviction.

- **Computer Crime & Intellectual Property Section** – The Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division has more than 30 attorneys and computer forensic experts that are specially trained in investigating and prosecuting high technology crime and intellectual property offenses, including issues relating to collection of electronic evidence.

- **Computer Hacking & Intellectual Property (CHIP) Program** – More than 200 specially trained Assistant U.S. Attorneys (AUSAs) in each of the 94 U.S. Attorneys offices are devoted to investigating and prosecuting computer crime and intellectual property offenses.

- **International Law** – The Department participated in the negotiation, and provided support for the ratification, of the international convention on cybercrime. This convention provides basic framework for substantive and procedural laws to allow greater cooperation among nations on the investigation and prosecution of cybercrime. The Department is also working with international agencies, particularly the Council of Europe, to increase the number of countries that are parties and to ensure the effective operation of the convention amongst its members.

- **International Law Enforcement Training** – The Department, in cooperation with other government agencies, trains foreign police, prosecutors and judges on techniques of investigating and prosecuting cybercrime and the importance of obtaining and preserving electronic evidence. Throughout the last year, Department attorneys have provided training in Russia and South

Africa, and provided regional training in sub-Sahara Africa and in Organization of American States countries.

- **International Law Enforcement Cooperation** – Through the operation of a 24/7 network and other operations, the Department seeks to maximize law enforcement cooperation through joint or parallel investigations with other nations.

- **Cybercrime and International Organized Crime** – The Department is working with select countries that are havens for cyber criminals targeting U.S. citizens and commerce. For example, as part of the International Organized Crime (IOC) strategy, the Department is working closely with law enforcement and prosecutors in Romania to target cyber thieves who prey on U.S. victims. A series of charges have been filed in Romania, with parallel charges in U.S. courts in California, Connecticut and Ohio.

Recent Prosecutions (CY 2008)

- *US v. E-Gold, et al.* – Recent guilty pleas by the digital currency organization, and its owners, that provided untraceable money transmitting used in credit card fraud, child exploitation and Ponzi schemes (District of Columbia).

Spam Prosecutions

- *US v. Soloway* – 47-month sentence for criminal spam scheme (Western District of Washington).

- *US v. Vitale* – 30-month sentence for criminal spam scheme (Southern District of New York).

- *US v. Ralsky, et al.* – Indictment for illegal spam used as part of financial fraud scheme (Eastern District of Michigan).

Online Frauds Affecting Financial Institutions

- *US v. Ramanathan* – Guilty plea to online hack/pump/dump scheme involving online brokerages (District of Nebraska).

- *US v. Davis* – 72-month sentence for falsifying account information from 11 financial institutions and 62 account holders (Western District of Texas).

- *US v. Holhoko, et al.* – Indictments in online extortion schemes affecting online brokerage firm (District of Montana).

- *US v. Simbaqueba* – 9-year sentence for using software to steal bank and payroll account usernames and passwords (Southern District of Florida).

- *US v. Largent* – Indictment to steal from online brokerage, involving opening more than 50,000 fictitious accounts (Eastern District of California).

Online Identity Thefts

- *US v. Sullivan* – 57-month sentence for stealing personal identity information of more than 5 million people (Middle District of Florida).

- *US v. Kalonji* – Indictment for stealing personal identity information of more than 150 persons from online gambling site (Southern District of New York).

- *US v. Brown* – 66-month sentence for identity theft relating to stolen credit card information (District of Arizona).

- *US v. Thompson, et al.* – Indictments of 11 persons for attempting to steal the identities of more than 50 people (Middle District of Louisiana).

Worms, Trojans, Botnets

- *US v. Milmont* – Guilty plea for operating an illegal botnet to spread worms (Central District of California).

- *US v. King* – Guilty plea for operating an illegal botnet to conduct denial of service attacks upon Internet commerce sites (Eastern District of California).

Online Fraud Schemes

- *US v. Carranza* – Indictment for money laundering regarding online fraud schemes (Eastern District of New York).

- *US v. Bently* – Conviction in online fraud scheme to illegally disseminate adware as part of online fraud scheme (Northern District of Florida).

Computer Intrusions to Steal Data or Damage Computers

- *US v. Oson* – 63 month sentence for hacking into health care clinic's computers to delete data (Southern District of California).

- *US v. Duann* – Indictment of former systems administrator for hacking into computer system used to track organ donors (Southern District of Texas).

- *US v. Munn* – Improper access by district attorney employee to obtain sensitive investigative database information for commercial use (Middle District of Louisiana).

# # #

08-693