United States Attorney's Office District of Connecticut
Press Release

May 19, 2008 **38 INDIVIDUALS IN U.S. AND ROMANIA CHARGED IN TWO RELATED CASES OF COMPUTER FRAUD INVOLVING INTERNATIONAL ORGANIZED CRIME**

International Law Enforcement Cooperation Leads to Disruption of Organized Crime Ring Operating in U.S. and Romania

BUCHAREST, ROMANIA – Thirty-eight individuals with ties to international organized crime have been charged in two separate indictments involving computer and credit card fraud schemes, Deputy Attorney General Mark R. Filip, Romanian Prosecutor General Laura Codruța Kövesi, U.S. Attorney for the Central District of California Thomas P. O'Brien and Acting U.S. Attorney for the District of Connecticut Nora R. Dannehy announced today. The Deputy Attorney General made the announcement with the Romanian Prosecutor General to highlight the extensive and continued cooperation between the two countries in addressing these types of international crimes. The announcement comes less than one month after U.S. Attorney General Michael B. Mukasey announced the Department's new Law Enforcement Strategy to Combat International Organized Crime.

"International organized crime poses a serious threat not only to the United States and Romania, but to all nations," said Deputy Attorney General Mark R. Filip. "Criminals who exploit the power and convenience of the Internet do not recognize national borders; therefore our efforts to prevent their attacks cannot end at our borders either. Through cooperation with our international partners, we can disrupt and dismantle these enterprises, just as we have done today with these indictments and arrests."

A federal grand jury in Los Angeles charged 33 individuals in a 65-count indictment unsealed today for their alleged participation in an international racketeering scheme that used the Internet to defraud thousands of individual victims and hundreds of financial institutions. Seven individuals were charged in a District of Connecticut indictment for their roles in an Internet phishing scheme, including two who were also charged in the Los Angeles case.

U.S. law enforcement authorities are executing nine arrest warrants in the Los Angeles area and Romanian law enforcement authorities are

executing search warrants in Romania today in connection with the racketeering indictment.

As described in the indictments and other publicly filed documents, a "phishing" scheme uses the Internet to target large numbers of unwary individuals, using fraud and deceit to obtain private personal and financial information such as names, addresses, bank account numbers, credit card numbers and Social Security numbers. Phishing schemes often work by sending out large numbers of counterfeit e-mail messages, which are made to appear as if they originated from legitimate banks, financial institutions or other companies.

The Los Angeles indictment alleges a conspiracy to violate the RICO Act; conspiracy in connection with access devices; production, use and trafficking in counterfeit access devices; bank fraud; aggravated identity theft; unauthorized access to a protected computer; possession of device making equipment; and a forfeiture allegation. The RICO conspiracy charge carries a maximum prison sentence of 20 years. The count of access device fraud conspiracy carries a maximum sentence of seven and a half years in prison; the charge of production, use and trafficking in counterfeit access devices carries a maximum 10 year prison sentence; and possession of device making equipment carries a 15 year maximum prison sentence. The charge of bank fraud carries a maximum 30 year prison sentence. The unauthorized access count carries a maximum prison sentence of five years, and aggravated identify theft carries a mandatory two year prison sentence. All charges except aggravated identity theft also contain provisions for fines and terms of supervised release.

According to the indictment, the Romania-based members of the enterprise obtained thousands of credit and debit card accounts and related personal information by phishing, with more than 1.3 million spam emails sent in one phishing attack. Once directed to a bogus site, victims were then prompted at those sites to enter access device and personal information. The Romanian “suppliers” collected the victims’ information and sent the data to U.S.-based “cashiers” via Internet “chat” messages. The domestic cashiers used hardware called encoders to record the fraudulently obtained information onto the magnetic strips on the back of credit and debit cards, and similar cards such as hotel keys. Cashiers then directed “runners” to test the fraudulent cards by checking balances or withdrawing small amounts of money at ATMs. The cards that were successfully tested, known as “cashable” cards, were used to withdraw money from ATMs or point of sale terminals that the cashiers had determined permitted the highest withdrawal limits. A portion of the proceeds was then wire transferred to the supplier who had provided the access device

information.

"Partnerships and cooperation among all levels of law enforcement – both domestic and foreign – are the keys to tackling criminal activity that increasingly knows no borders," said U.S. Attorney for the Central District of California Thomas P. O'Brien. "Just as street gangs don't respect municipal borders, computer criminals can reach into other countries and prey upon unsuspecting victims who have no idea their identities and money are going to another country."

The individuals named in the indictment operated from locations in the United States and abroad including Canada, Pakistan, Portugal and Romania, and include both U.S. citizens and foreign nationals. Sonny Duc Vo, Alex Chung Luong and Leonard Gonzales are U.S. citizens. Nga Ngo, Thai Hoang Nguyen, Loi Tan Dang and Dung Phan are permanent legal residents of Vietnam. Hiep Thanh Tran is a U.S. permanent resident from Vietnam. Caroline Tath is a permanent legal resident of Cambodia. Hassan Parvez is a citizen of Pakistan. Rolando Soriano is a Mexican citizen and is currently charged in Los Angeles with illegal entry by an alien following deportation. Ovidiu-Ionut Nicola-Roman; Petru Bogdan Belbita; Stefan Sorin Ilinca; Sorin Alin Panait; Costel Bulugea; Nicolae Dragos Draghici; Florin Georgel Spiru; Marian Daniel Ciulean; Irinel Nicusor Stancu; Didi Gabriel Constantin; Mihai Draghici; Marius Sorin Tomescu; Lucian Zamfirache; Laurentiu Cristian Busca; Dan Ionescu; Marius Lnu; Alex Gabriel Paralescu; and Andreea Nicoleta Stancuta are Romanian citizens. An additional four individuals known only by their aliases, "Cryptmaster"; "PaulXSS"; "euro_pin_atm" and "SeleQtor" are believed to be Romanian citizens.

Seuong Wook Lee, a cashier in the scheme, pleaded guilty on May 15, 2008, in U.S. District Court in Los Angeles to racketeering conspiracy, bank fraud, access device fraud and unauthorized access of a protected computer.

In a related case, seven Romanian citizens were charged in an indictment returned by a federal grand jury in New Haven, Conn., on Jan. 18, 2007, and unsealed on May 16, 2008, in connection with an Internet phishing scheme. The indictment alleges conspiracy to commit fraud in connection with access devices, conspiracy to commit bank fraud and aggravated identity theft.
The investigation in the District of Connecticut resulted from a citizen's complaint concerning a fraudulent e-mail message made to appear as if it originated from Connecticut-based People's Bank. In fact, the e-mail message directed victims to a computer in Minnesota that had been compromised, or "hacked," and used to host a

counterfeit People's Bank Internet site. During the course of the investigation, it was determined that the individuals had engaged in similar phishing schemes against many other financial institutions and companies, including Citibank, Capital One, JPMorgan Chase & Co., Comerica Bank, Wells Fargo & Co., eBay and PayPal.

"This case shows that Internet fraudsters cannot avoid prosecution just by launching their attacks against U.S. residents and U.S. companies from overseas," said Acting U.S. Attorney for the District of Connecticut Nora R. Dannehy. "With the help of our law enforcement partners around the world, we will investigate and prosecute fraudsters wherever they can be found."

"We will continue to work closely with our foreign and domestic law enforcement partners and employ the investigative tools available to bring organized criminals to justice," said FBI Deputy Director John S. Pistole. "The recent cooperation and information sharing with our Romanian law enforcement partners and allies at the Southeast European Cooperative Initiative has been invaluable. Despite being separated by oceans, we are united in the fight against organized crime."

The individuals named in the District of Connecticut indictment are Ciprian Dumitru Tudor, Ovidiu-Ionut Nicola-Roman, Mihai Cristian Dumitru and Petru Bogdan Belbita, all residents of Craiova, Romania; and Radu Mihai Dobrica, Cornel Ionut Tonita and Cristian Navodaru, all residents of Galati, Romania. Nicola-Roman was located in Bulgaria and arrested on an Interpol warrant on June 6, 2007. He was extradited to the United States on Nov. 8, 2007. Nicola-Roman and Belbita are also charged in the Los Angeles case.

If convicted, each of the individuals in the District of Connecticut case faces a maximum term of five years in prison on each conspiracy charge, and a mandatory term of two years in prison on the aggravated identify theft charge. In addition, each of the individuals is subject to a maximum fine of $250,000 on each count, or twice the gain resulting from the offense, whichever is greater. The individuals also may be sentenced to a maximum term of three years supervised release on each charge.

On April 23, 2008, Attorney General Michael B. Mukasey announced the Law Enforcement Strategy to Combat International Organized Crime to address the growing threat to U.S. security and stability posed by international organized crime. The strategy was developed following an October 2007 International Organized Crime Threat

Assessment.

The strategy specifically reacts to the globalization of legal and illegal business, advances in technology, particularly the Internet, and the evolution of symbiotic relationships between criminals, public officials and business leaders that have combined to create a new, less restrictive environment within which international organized criminals can operate. Without the necessity of a physical presence, U.S. law enforcement must combat international organized criminals that target the relative wealth of the people and institutions in the United States while remaining outside the country. Ultimately, the strategy aims to create consensus among domestic law enforcement in identifying the most significant priority targets and then unified and concerted action among domestic and international law enforcement in significantly disrupting and dismantling those targets.

International organized crime is defined as those self-perpetuating associations of individuals who operate internationally for the purpose of obtaining power, influence, monetary and commercial gains, wholly or in part by illegal means, while protecting their activities through a pattern of corruption and violence. International organized criminals operate in hierarchies, clans, networks and cells. The crimes they commit vary as widely as the organizational structures they employ.

An indictment is a formal charging document notifying the defendant of his/her charges. All persons charged in an indictment are presumed innocent until proven guilty.

The Los Angeles case is the result of a joint investigation involving the FBI, the Romanian General Inspectorate of Police, the U.S. Postal Service, the Internal Revenue Service and local law enforcement agencies including the Seal Beach, Costa Mesa, Huntington Beach, Irvine, Westminster and Anaheim, Calif., Police Departments. Additional assistance was provided by the U.S. Secret Service. The case is being prosecuted by Assistant U.S. Attorney Mark Aveis in the U.S. Attorney's Office for the Central District of California.

The case being prosecuted in the District of Connecticut was investigated by the FBI and the Connecticut Computer Crimes Task Force. The case is being prosecuted by Assistant U.S. Attorney Edward Chang of the U.S. Attorney Office's Computer Hacking and Intellectual Property Unit.

CONTACT: **U.S. ATTORNEY'S OFFICE**
Tom Carson
(203) 821-3722
thomas.carson@usdoj.gov