November 13, 2007
CRM
(202) 514-2008
TDD (202) 514-1888
WWW.USDOJ.GOV

Romanian Authorities Arrest 9 of 22 Defendants Charged in Organized Crime Group

21 Simultaneous Searches Reveal Evidence of Massive "Phishing" and Fraud Scheme

The press office of the Prosecutor's Office by the High Court of Cessation and Justice is authorized to bring to the attention of the public the following:

On November 13, 2007 Prosecutors from the Directorate for Investigating Organized Crime and Terrorism arrested 9 of the 22 persons who were charged for the crimes of setting up an organized criminal group, computer fraud, fraudulent use of electronic payment instruments, and production and maintenance of equipment needed to counterfeit electronic payment instruments.

In March of this year investigators received information that massive fraudulent transactions using stolen credit cards were taking place on the Western Union system in several Romanian counties. In April 2007, a bank notified Romanian authorities that if had been the target of "phishing" attacks. By means of data provided by the bank, other victim financial institutions abroad were identified which had also been "phished."

Electronic monitoring and physical surveillance of the criminal group identified the subjects' specialties and their advanced computer knowledge. The investigation established the group's methods, as follows:

- use of specialized software for "phishing" attacks against banks abroad;
- collection of identification data from electronic payments instruments (names of holders, credit cards, pin code, etc.)
- fraudulent use of data and creation of cloned credit cards;
- financial transfers via the Western Union payment system and physical withdrawals from ATMs;
- collection of identification data from credit cards through "skimming" (the use of devices to physically copy of the magnetic strips on credit cards).

On November 13, 2007, 21 simultaneous searches were performed at locations in Bucharest and Constanta, Romania, resulting in the identification of computer systems used to commit the crimes, electronic equipment, false ATM "faces", card reading and writing devices, blank cards, etc.

Losses estimated so far over two months total approximately $130,000.

The dismantlement of this organized crime network was the result of close cooperation with the US Department of Justice and FBI through its Legal Attache in Bucharest, together with police officers of the General Directorate for Combating Organized Crime and the Constanta Brigade for Combating Organized Crime, supported by the fighters of Romanian Gendarmerie.

###

November 5, 2007
United States Attorney
Western District of Washington
700 Stewart Street, Suite 5220
Seattle, Washington 98101-1271
Tel: (206) 553-7970
Fax: (206) 553-0882

Seattle Man Pleads Guilty in Connection with ID Theft Using Computer File Sharing Programs

First Conviction in the Country Involving Peer to Peer File Sharing Programs

GREGORY KOPILOFF, 35, of Seattle, Washington, pleaded guilty this morning in U.S. District Court in Seattle to Mail Fraud, Accessing a Protected Computer without Authorization to Further Fraud and Aggravated Identity Theft. In his plea agreement KOPILOFF admits he used file sharing programs to invade the computers of victims across the United States to get access to their personal information in tax returns, credit reports, bank statements and student financial aid applications. KOPILOFF admits in his plea agreement that he used the personal information of more than 50 people to commit his fraud. KOPILOFF used the information to fraudulently purchase and resell more than $73,000 in merchandise.

According to the plea agreement, KOPILOFF used peer to peer file sharing programs, which are most commonly known for their use in replicating copyright protected music and videos, to commit his fraud. Using peer to peer programs, including "Limewire," KOPILOFF could "search" the computers of others who were part of the file sharing "network" for federal income tax returns, student financial aid applications, and credit reports that had been stored electronically by other real people on and in their own private computers. KOPILOFF would download those documents onto his own computer, and would then use the identity, and banking, financial, and credit information to open credit accounts over the Internet, in the names of the other real people whose identities he had stolen. KOPILOFF would make fraudulent online purchases of merchandise, have it shipped to various mailboxes in the Puget Sound area, and then would sell the merchandise for about half its retail value. KOPILOFF also used personal information he obtained by more traditional methods such as stealing mail or taking records from trash cans.

KOPILOFF will be sentenced by U.S. District Judge James L. Robart on January 28, 2008. Mail Fraud is punishable by up to 20 years in prison, and a $250,000 fine. Accessing a Protected Computer without Authorization to Further Fraud is punishable by up to 5 years in prison and a

$250,000 fine. A conviction for Aggravated Identity Theft mandates a two year prison sentence to run consecutive to the prison time imposed on the underlying conviction.

The case was investigated by the Electronic Crimes Task Force of the U.S. Secret Service, the U.S. Postal Inspection Service, the Seattle Police Department and Poulsbo Police Department.

The case is being prosecuted by Assistant United States Attorney Kathryn Warma of the Computer Hacking and Internet Crimes (CHIPS) Unit of the United States Attorney's Office.

For additional information please contact Emily Langlie, Public Affairs Officer for the United States Attorney's Office, at (206) 553-4110.