U.S. Department of Justice

United States Attorney
District of Connecticut

Connecticut Financial Center *(203) 821-3700*
157 Church Street *Fax (203) 773-5376*
New Haven, Connecticut 06510 *www.justice.gov/usao/ct*

December 22, 2011

FOURTEEN CITIZENS OF ROMANIA CHARGED WITH PARTICIPATING IN INTERNET PHISHING SCHEME

David B. Fein, United States Attorney for the District of Connecticut, and Kimberly K. Mertz, Special Agent in Charge of the Federal Bureau of Investigation, today announced the unsealing of an indictment charging 14 Romanian citizens with conspiracy, fraud and identity theft offenses stemming from their alleged participation in an extensive Internet "phishing" scheme.

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.

Charged in the indictment are **CIPRIAN DUMITRU TUDOR**, **MIHAI CRISTIAN DUMITRU**, **BOGDAN BOCEANU**, **BOGDAN-MIRCEA STOICA**, **OCTAVIAN FUDULU**, **IULIAN SCHIOPU**, **RAZVAN LEOPOLD SCHIBA**, **DRAGOS RAZVAN DAVIDESCU**, **ANDREI BOLOVAN**, **LAURENTIU CRISTIAN BUSCA**, **GABRIEL SAIN**, **DRAGOS NICOLAE DRAGHICI**, **STEFAN SORIN ILINCA** and **MIHAI ALEXANDRU DIDU**, all residents of Romania.

The indictment alleges that, in June 2005, one or more defendants sent a spam email to individuals, including a resident of Madison, Conn., which purported to be from Connecticut-based People's Bank. The email stated that the recipient's online banking access profile had been locked and instructed recipients to click on a link to a web page where they could enter information to "unlock" their profile. The web page appeared to originate from People's Bank, but was actually hosted on a compromised computer unrelated to People's Bank. Any personal identifying and financial information provided by the individual would be sent by email to one or more of the defendants or to a "collector" account, which was an email account used to receive and collect the information obtained through phishing.