NEWS RELEASE

OFFICE OF THE UNITED STATES ATTORNEY
SOUTHERN DISTRICT OF CALIFORNIA
San Diego, California

United States Attorney
Karen P. Hewitt

For Further Information, Contact: Assistant U. S. Attorney Mitch Dembin, 619-557-5558

For Immediate Release

NEWS RELEASE SUMMARY - December 8, 2009

United States Attorney Karen P. Hewitt announced that Jeffrey Steven Girandola and Kajohn Phommavong have been charged in a previously sealed 16-count indictment handed up by a federal grand jury on November 20, 2009, with Conspiracy, Computer Fraud, Access Device Fraud and Aggravated Identity Theft. The indictment was unsealed upon the initial appearance of Mr. Phommavong today before United States Magistrate Judge Nita L. Stormes, in federal court in San Diego. Mr. Girandola is presently in custody in San Diego County on other charges.

According to the indictment, the defendants installed peer-to-peer file sharing software on computers under their control and searched the available peer-to-peer file sharing networks for account login information and passwords inadvertently exposed to the file sharing network by other users of the peer-to-peer file sharing software. Peer-to-peer or "P2P" software programs, the indictment explains, allow users to share files and other data with other users of that software. Most P2P software is free and available to download to anyone with a computer and an Internet connection. After installation, the user can search all files made available

for sharing by any other users of that program and download files of interest. Users can place files that the user wants to share into a folder on the user's computer designated for sharing. It is not unusual, however, for users to download corrupt P2P programs or to misconfigure the software and unintentionally allow all of the files on their computer to be shared to the community.

The defendants are charged with using the account information and passwords that they obtained by searching the P2P networks to access the bank accounts of the victims and transfer funds to prepaid credit cards which they obtained in their own names. The defendants are alleged to have used the prepaid credit cards to purchase goods and to obtain cash in and around San Diego County. The victims include five users of the online payroll system of the United States Department of Defense ("DoD"). DoD, through its Defense Finance and Accounting Service ("DFAS") provides an Internet accessible website to DoD personnel, including the Armed Forces, known as "DFAS MyPay," to view and change information relating to their paychecks and other benefits. According to the indictment, the defendants accessed the accounts of the five individuals, consisting of active duty military, retired military and a civilian employee of the Air Force, Navy and Marine Corps, and re-directed their paychecks to the defendants' prepaid credit card accounts. The defendants also are charged with victimizing a company in Florida that is in the business of selling products to assist senior citizens. All together, during the commission of these offenses from November 22, 2005, until September 12, 2006, according to the indictment, the defendant redirected and attempted to redirect over $20,000 in funds to themselves.

Bail was set at $20,000 for Mr. Phommavong. His next appearance will be on January 8, 2010, before United States District Judge Jeffrey T. Miller for hearing motions and setting a trial date. Mr. Girandola's appearance will be arranged with the County of San Diego.

This case was investigated by Special Agents of the Cybersquad of Federal Bureau of Investigation in San Diego and by Special Agents of the Defense Criminal Investigative Service.

DEFENDANTS **Case Number: 09cr4205JM**

Jeffrey Steven Girandola
Kajohn Phommavong

SUMMARY OF CHARGES

Count 1: Title 18, United States Code, Section 371 - Conspiracy
Maximum Penalty: 5 years' imprisonment and $250,000 fine

Counts 2-10: Title 18, United States Code, Section 1030(a)(4) - Computer Fraud
Maximum Penalty: 5 years' imprisonment and $250,000 per count

Count 11: Title 18, United States Code, Section 1029(a)(2) and (b)(1) - Access Device Fraud
Maximum Penalty: 10 years' imprisonment and $250,000

Counts 12-16: Title 18, United States Code, Section 1028A - Aggravated Identity Theft
Maximum Penalty: Mandatory sentence of 2 years consecutive to any other sentence

AGENCIES

Federal Bureau of Investigation
Defense Criminal Investigative Service

An indictment itself is not evidence that the defendants committed the crimes charged. The defendants are presumed innocent until the Government meets its burden in court of proving guilt beyond a reasonable doubt.