NEWS RELEASE

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

United States Attorney
Laura E. Duffy

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

For Immediate Release

NEWS RELEASE SUMMARY - July 9, 2010

United States Attorney Laura E. Duffy announced that Jeffrey Steven Girandola and Kajohn Phommavong were sentenced today by United States District Judge Jeffrey T. Miller based upon their prior guilty pleas to federal identity theft charges. Judge Miller sentenced Mr. Girandola to serve 32 months imprisonment, and Mr. Phommavong was sentenced to serve two months in federal prison followed by a four-month commitment to a halfway house.

On April 13, 2010, Mr. Girandola pleaded guilty to one count each of computer fraud, access device fraud and aggravated identity theft. Mr. Phommavong, on the same day, pleaded guilty to one count of conspiracy to commit computer fraud and access device fraud. In connection with their guilty pleas, as charged in the indictment, the defendants admitted that they 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 admitted 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 then 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. The defendants admitted accessing 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 admitted 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.

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

Title 18, United States Code, Section 371 - Conspiracy

Title 18, United States Code, Section 1030(a)(4) - Computer Fraud

Title 18, United States Code, Section 1029(a)(2) and (b)(1) - Access Device Fraud

Title 18, United States Code, Section 1028A - Aggravated Identity Theft

AGENCIES

Federal Bureau of Investigation
Defense Criminal Investigative Service