For Immediate Release
October 7, 2009

FBI Los Angeles
Contact: Public Affairs Specialist Laura Eimiller
(310) 996-3343

One Hundred Linked to International Computer Hacking Ring Charged by United States and Egypt in Operation Phish Phry

LOS ANGELES—The largest number of defendants ever charged in a cyber crime case have been indicted in a multinational investigation conducted in the United States and Egypt that uncovered a sophisticated "phishing" operation that fraudulently collected personal information from thousands of victims that was used to defraud American banks.

This morning, authorities in several United States cities arrested 33 of 53 defendants named in an indictment returned last week by a federal grand jury in Los Angeles. Several defendants charged in the indictment are being sought this morning by law enforcement. Additionally, authorities in Egypt have charged 47 defendants linked to the phishing scheme. The United States government is extremely grateful for the extraordinary assistance provided by the Egyptian government in this matter.

Operation Phish Phry marks the first joint cyber investigation between Egyptian law enforcement authorities and United States officials, which include the FBI, the United States Attorney's Office, and the Electronic Crimes Task Force in Los Angeles. Phish Phry, with 53 defendants charged in United States District Court, also marks the largest cyber crime investigation to date in the United States.

Operation Phish Phry was announced following this morning's arrests by Keith B. Bolcar, Acting Assistant Director in Charge of the FBI in Los Angeles; George S. Cardona, Acting United States Attorney in Los Angeles; Kieran Ramsey, the FBI's Legal Attache in Cairo, Egypt; and Egyptian Law Enforcement Authorities.

Operation Phish Phry commenced in 2007 when FBI agents, working with United States financial institutions, took proactive steps to identify and disrupt sophisticated criminal enterprises targeting the financial infrastructure in the United States. Intelligence developed during the initiative prompted the FBI and Egyptian authorities to agree to pursue a joint investigation into multiple subjects based in Egypt after investigators in both countries earlier this year uncovered an international conspiracy allegedly operating an elaborate scheme to steal identities through a method commonly called "phishing." The group is accused of conspiring to target American-based financial institutions and victimize an unknown number of account holders by fraudulently using their personal financial information.

The multinational investigative effort resulted in 53 defendants being named in the federal indictment and 47 suspects being identified by Egyptian authorities. The domestic defendants were arrested in California, Nevada, and North Carolina. In California,

defendants reside in the counties of Los Angeles, Orange, San Bernardino, Riverside, and San Diego.

The 51-count indictment accuses all of the defendants with conspiracy to commit wire fraud and bank fraud. Various defendants are charged with bank fraud; aggravated identity theft; conspiracy to commit computer fraud, specifically unauthorized access to protected computers in connection with fraudulent bank transfers and domestic and international money laundering.

According to the indictment that was unsealed this morning, Egyptian-based hackers obtained bank account numbers and related personal identification information from an unknown number of bank customers through phishing—a technique that involves sending e-mail messages that appear to be official correspondence from banks or credit card vendors. In illegal phishing schemes, bank customers are directed to fake websites purporting to be linked to financial institutions, where the customers are asked to enter their account numbers, passwords and other personal identification information. Because the websites appear to be legitimate—complete with bank logos and legal disclaimers—the customers do not realize that the websites do not belong to legitimate financial institutions.

The indictment alleges that co-conspirators in Egypt collected victims' bank account information by using information obtained from their phishing activities. Armed with the bank account information, members of the conspiracy hacked into accounts at two banks. Once they accessed the accounts, the individuals operating in Egypt communicated via text messages, telephone calls and Internet chat groups with co-conspirators in the United States. Through these communications, members of the criminal ring coordinated the illicit online transfer of funds from compromised accounts to newly created fraudulent accounts. The United States part of the ring was allegedly directed by defendants Kenneth Joseph Lucas, Nichole Michelle Merzi, and Jonathan Preston Clark, all California residents, who directed trusted associates to recruit “runners,” who set up bank accounts where the funds stolen from the compromised accounts could be transferred and withdrawn. A portion of the illegally obtained funds withdrawn were then transferred via wire services to the individuals operating in Egypt who had originally provided the bank account information obtained via phishing.

"The sophistication with which Phish Phry defendants operated represents an evolving and troubling paradigm in the way identity theft is now committed," said Keith Bolcar, Acting Assistant Director In Charge of the FBI in Los Angeles. "Criminally savvy groups recruit here and abroad to pool tactics and skills necessary to commit organized theft facilitated by the computer, including hacking, fraud and identity theft, with a common greed and shared willingness to victimize Americans. The FBI is grateful for the assistance of its law enforcement partners in the U.S. and the Egyptian government's dedicated cooperation, which illustrates that borders cease to exist among countries committed to the rule of law and to the protection of their citizens."

Acting United States Attorney George S. Cardona stated: “This international phishing ring had a significant impact on two banks and caused huge headaches for hundreds, perhaps thousands, of bank customers. Organized, international criminal rings can only be confronted by an organized response by law enforcement across international borders, which we have seen in this case.”

Those taken into custody in the United States will be afforded an initial appearance before United States Magistrate Judges in the district where they were arrested. Those arrested in and around Los Angeles will have their initial appearance in United States District Court in Los Angeles this afternoon.

Each of the 53 defendants named in the indictment is charged with conspiracy to commit bank fraud and wire fraud, a charge that carries a statutory maximum penalty of 20 years in federal prison. Some of the defendants are named in additional counts that would increase their maximum possible sentences.

An indictment contains allegations that a defendant has committed a crime. Every defendant is presumed to be innocent until and unless proven guilty in court.

The investigation in the United States was conducted by the FBI’s Los Angeles Field Office, supported by the Electronic Crimes Task Force in Los Angeles and the FBI’s Legal Attache in Cairo, Egypt. Several agencies provided considerable assistance to this investigation, including the Los Angeles Police Department, the Los Angeles District Attorney, the United States Secret Service, the Culver City Police Department, the El Segundo Police Department, and the United States Social Security Administration. U.S. Customs and Border Protection, the Drug Enforcement Administration, the Department of Water and Power, and local law enforcement departments in various counties assisted during today’s arrests.

The defendants charged in the United States will be prosecuted by the United States Attorney’s Office. The Department of Justice Criminal Division's Office of International Affairs provided substantial support during the investigation.

MEDIA CONTACT:
FBI: Laura Eimiller - (310) 996-3343
U.S. Attorney’s Office: Thom Mrozek - (213) 894-6947