NEWS RELEASE

For Immediate Distribution

March 25, 2011

André Birotte Jr.
United States Attorney
Central District of California

Thom Mrozek, Public Affairs Officer
(213) 894-6947
thom.mrozek@usdoj.gov
www.justice.gov/usao/cac

FIVE DOMESTIC DEFENDANTS LINKED TO INTERNATIONAL COMPUTER HACKING RING GUILTY OF FEDERAL FRAUD CHARGES

46 People Charged in Operation 'Phish Phry' Have Now Been Convicted

LOS ANGELES – Five people were convicted today of federal charges for their roles in an international "phishing" operation that used spam emails and bogus websites to collect personal information that was used to defraud American banks.

The five found guilty this afternoon by a federal jury were among 53 defendants charged in the fall of 2009 as part of Operation "Phish Phry," a multinational investigation conducted in the United States and Egypt that led to charges against 100 individuals – the largest number of defendants ever charged in a cybercrime case. With today's guilty verdicts, 46 people have been convicted in federal court in Los Angeles as a result of Phish Phry.

Operation Phish Phry revealed how 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. Bank customers who received the spam emails were directed to fake websites purporting to be linked to financial institutions, where the customers were asked to enter their account numbers, passwords and other personal identification information. Because the websites appeared to be legitimate – complete with bank logos and legal disclaimers – the victims did not realize that the websites were not related to legitimate

financial institutions.

Members of the conspiracy 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 chats with co-conspirators in the United States. Through these communications, members of the criminal ring coordinated the illicit online transfer of funds from the compromised accounts to newly created fraudulent accounts.

The United States part of the ring was directed by three people, including Nichole Michelle Merzi, one of the defendants who was convicted today. The leaders of the domestic part of the scheme directed associates to recruit runners to 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 Egyptian co-conspirators who had originally provided the bank account information obtained via phishing.

The defendants found guilty today were:

- Nichole Michelle Merzi, 25, of Oceanside, who was found guilty of conspiracy, computer fraud, bank fraud and aggravated identity theft;
- Tramond S. Davis, 21, of Las Vegas, Nevada, who was found guilty of conspiracy;
- Shontovia D. Debose, 22, of Las Vegas, Nevada, who was found guilty of conspiracy;
- Anthony Donnel Fuller, 22, of Corona, who was found guilty of conspiracy and two counts of bank fraud; and
- Me Arlene Settle, 22, of Garden Grover, who was found guilty of conspiracy and two counts of bank fraud.

The five defendants are scheduled to by sentenced by United States District Judge Valerie Baker Fairbank on October 31.

Along with Merzi, the two other leaders of the domestic branch of the phishing scheme were Kenneth Joseph Lucas, 26, of Los Angeles, and Jonathan Preston Clark,

26, of Los Angeles. Lucas previously pleaded guilty to conspiracy, bank fraud and aggravated identity theft, and he is scheduled to be sentenced on June 22. Clark previously pleaded guilty to conspiracy and bank fraud, and he is expected to appear for sentencing before Judge Fairbank on June 8.

The conspiracy and bank fraud charges in this case carry statutory maximum sentences of 30 years in federal prison. The charge of aggravated identity theft carries a minimum sentence of two years that must be added to any of sentence imposed on the defendant.

The jury that convicted the five defendants today determined that one defendant was not guilty. One defendant has agreed to plead guilty, and one defendant is a fugitive. Prosecutors previously dismissed charges against two of the defendants initially charged in this case. The final two defendants charged in relation to Phish Phry are pending trial.

The investigation in the United States was conducted by the Federal Bureau of Investigation, which received support from the Electronic Crimes Task Force in Los Angeles and the Social Security Administration's Office of Special Investigations.

CONTACT: Assistant United States Attorney Ronald Cheng
Cyber and Intellectual Property Crimes Section
(213) 894-8644

Assistant United States Attorney Mark Krause
Cyber and Intellectual Property Crimes Section
(213) 894-3493

Release No. 11-045