NEWS RELEASE

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

For Immediate Distribution

June 27, 2011

LEAD DEFENDANT IN INTERNATIONAL COMPUTER HACKING RING SENTENCED IN TWO CASES TO 13 YEARS IN FEDERAL PRISON

Los Angeles Man also Sentenced for Marijuana Grow Seen on YouTube

LOS ANGELES – Federal judges in two cases have imposed sentences totaling 13 years in prison against a Los Angeles man who was the leader of the domestic arm of an international "phishing" operation that used spam emails and bogus websites to collect personal information that was used to defraud American banks.

Kenneth Joseph Lucas, II, 27, was sentenced this afternoon in the second case, which involved an indoor marijuana grow at his residence in the Baldwin Hills district of Los Angeles.

In relation to the narcotics case, United States District Judge Gary A. Feess sentenced Lucas this afternoon to five years in prison – with two years of that sentence to run consecutively to an 11-year sentence imposed last week in the phishing case. Judge Feess observed that Lucas' conduct spanning both cases was "astonishing" and that Lucas caused "great harm to many people."

In the case stemming from the phishing scheme, United States District Judge Valerie Baker Fairbank sentenced Lucas on Friday to 11 years in prison after he pleaded guilty to 49 counts of bank and wire fraud, aggravated identity theft, computer fraud, and money laundering conspiracy charges.

During Friday's sentencing hearing, Judge Fairbank said that Lucas' role in the phishing scheme was "deliberate and ongoing," and that his actions showed an

“extreme disregard for the law and the community.” Lucas was a “key and active player in the bank fraud” that extended from Southern California to Nevada, North Carolina, Maryland, and overseas in Egypt, Judge Fairbank said.

In total, Lucas has been sentenced to 156 months in federal prison.

Lucas was the lead defendant in a 53-defendant indictment returned 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. As a result of Operation Phish Phry, 47 people have been convicted in federal court in Los Angeles.

Operation Phish Phry revealed how Egyptian 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. Armed with the bank account information, members of the conspiracy hacked into accounts at two banks. Once they accessed the accounts, the individuals in Egypt coordinated transfers of funds from the compromised accounts to newly created fraudulent accounts and other accounts used as part of the scheme.

The United States part of the ring was directed by Lucas and two others, who directed associates to recruit runners to set up and use bank accounts where stolen funds could be held. A portion of the illegally obtained funds were transferred via wire services to the Egyptian co-conspirators. Judge Fairbank determined the total amount of intended loss was more than $1 million.

In the narcotics case, Lucas oversaw the construction of an indoor marijuana grow operation at his residence in 2009. After installing an irrigation system, ventilation equipment, indoor lights and fans, Lucas posted videos on YouTube that showcased the grow operation. On October 7, 2009, authorities found 100 marijuana plants in the

grow room, and Lucas admitted to having grown and sold a prior crop, which netted him $45,000.

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

Release No. 11-092