NEWS RELEASE

For Immediate Distribution

December 18, 2007

Thomas P. O'Brien
United States Attorney
Central District of California

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

L.A. COUNTY MAN PLEADS GUILTY TO HACKING INTO HOTEL BUSINESS KIOSKS AND STEALING CREDIT CARD INFORMATION

A Lomita man pleaded guilty this afternoon to federal charges stemming from his hacking into business kiosks at hotels and stealing credit card information.

Hario Tandiwidjojo, 28, pleaded guilty to one count of unauthorized access to a protected computer to conduct fraud.

In a plea agreement filed in United States District Court, Tandiwidjojo admitted that he hacked into approximately 60 computers inside business kiosks operated by Showcase Business Centers, Inc. Tandiwidjojo bypassed four password checks that Showcase Business Centers had in place on their computers, using passwords he obtained while employed by a company that serviced the business kiosks. After hacking into the computers, Tandiwidjojo installed malicious software that allowed him to intercept data, such as credit card information from customers who used the business kiosks. The malicious software that Tandiwidjojo had installed transferred the stolen customer data to a website he controlled. Tandiwidjojo then used this information to fraudulently make charges to the stolen credit card accounts.

Tandiwidjojo's activities led to $34,266 in losses in only three days in February 2007.

When FBI agents searched Tandiwidjojo's residence in August, they discovered a credit card writer that is used to put information on magnetic strips on

credit cards, a credit card terminal used to process credit card transactions, multiple bank and gift cards, and a California driver's license with Tandiwidjojo's picture but another name.

Tandiwidjojo pleaded guilty before United States District Judge Gary A. Feess, who is scheduled to sentence the defendant on March 3. At sentencing, Tandiwidjojo faces a statutory maximum penalty of five years in federal prison, although the plea agreement contemplates a sentence in the range of 10 months to 16 months.

This case was the result of an investigation by the Federal Bureau of Investigation.

CONTACT: Assistant United States Attorney Erik M. Silber
Cyber and Intellectual Property Crimes Section
(213) 894-2231

Assistant United States Attorney Rozella A. Oliver
Cyber and Intellectual Property Crimes Section
(213) 894-2475

Release No. 07-161