



**United States Department of Justice
United States Attorney's Office
District of Minnesota**

**Frank J. Magill,
United States Attorney**

David Anderson, Public Affairs Specialist
(612) 664-5684; cell: (612) 730-2251

News Release

FOR IMMEDIATE RELEASE
Tuesday, May 5, 2009

2 indicted for aggravated identity theft, conspiracy

Two men were indicted today in federal court in connection with an alleged scheme to fraudulently obtain cash and property by using stolen access devices, namely credit cards to purchase Visa gift cards and obtain money and things of value.

Ion Datcu, 51, Seattle, and Stelian Cipu, 31, Bucharest, Romania, were each charged with one count of conspiracy to commit access device fraud, one count of aggravated identity theft, one count of access device fraud and one count of possession of device-making equipment. Datcu was also charged with an additional count of access device fraud.

Their indictment alleges that the defendants possessed 15 or more access devices that are counterfeit and unauthorized.

The defendants allegedly would obtain lost or stolen credit cards. Then they would allegedly attach a "skimming device" to ATMs in order to secretly capture the magnetic access device data from credit/debit cards of innocent ATM users. Next, they would allegedly use a magnetic strip writer to alter the stolen cards by re-encoding them with the skimmed information. In this way, the access device data contained on the card's magnetic strip would not match the cardholder's name, and therefore, could still be used even though the card may have been reported lost or stolen.

In furtherance of the conspiracy, on March 11 the defendants traveled in a rented vehicle from Seattle to Minnesota, and on March 13 rented a hotel room in Maplewood. On March 14 and 15, the defendants allegedly attached a skimming device to an ATM at a TCF Bank in Maplewood and obtained unauthorized access device data belonging to customers who used the ATM.

Also on March 15, the defendants knowingly possessed and used, without lawful authority, credit cards issued to 17 victims, and knowingly possessed lost or stolen credit cards bearing the names of those 17 victims. The defendants also knowingly possessed a laptop computer containing access device data, a magnetic strip card reader/writer and one magnetic card skimming device.

According to a United States Secret Service affidavit, on March 15 a citizen notified the Maplewood Police Department regarding two suspicious men walking from the TCF Bank to a nearby Bremer Bank. Police stopped the two men, later identified as Datcu and Cipu, and recovered a credit card in Datcu's pocket in the name of a Seattle woman that was reported lost or stolen. They also recovered a credit card in Cipu's wallet in the name of a Seattle man that was reported lost or stolen.

In their vehicle, police recovered seven credit cards, six of which were reported stolen out of the Seattle area, as well as a list of eight retail malls in Minnesota and Wisconsin, and a computer bag that contained a wig, screwdriver, razor knife and nine credit cards that had been reported lost or stolen out of Seattle. Both men were arrested for possession of theft tools.

During the execution of a search warrant of the defendants' hotel room, police recovered 47 Visa gift cards, a portable credit card scanner, a magnetic card strip reader, a thumbdrive electronic storage device and a laptop computer. Police discovered that the access device data of the recovered credit cards had been altered.

During a search of the computer, authorities found access device account numbers from 230 separate accounts.

"This case illustrates the importance of closely scrutinizing credit card statements at the end of each billing cycle," said John Kirkwood, Special Agent in Charge of the U.S. Secret Service's Minneapolis District Office. "It is also important to closely inspect ATM machines to assure no foreign device or "skimmer" has been placed over the card reader slot. It is important for sales clerks to closely compare the embossed name and card number on the front of the card, with the displayed information from the electronic magnetic strip off the back of the credit card."

If convicted, both defendants face a potential maximum penalty of five years in prison on the conspiracy count, 20 years on the possession of device-making equipment count and a mandatory two-year minimum penalty on the aggravated identity theft count. Datcu also faces a potential maximum penalty of 20 years on each of the access device fraud counts, while Cipu also faces a potential maximum penalty of 10 years on the access device fraud count. All sentences are determined by a federal district court judge.

This case is the result of an investigation by the Maplewood Police Department and the U.S. Secret Service. It is being prosecuted by Assistant U.S. Attorney Lisa D. Kirkpatrick.

An indictment is a determination by a grand jury that there is probable cause to believe that offenses have been committed by a defendant. A defendant, of course, is presumed innocent until he or she pleads guilty or is proven guilty at trial.