

Identity Thieves Organize

*Investigators See New Pattern:
Criminals Team Up to Sell
Stolen Data Over the Internet*

By CASSELL BRYAN-LOW
Staff Reporter of THE WALL STREET JOURNAL
April 7, 2005; Page B1

Recent investigations of online identity-theft rings show a disturbing pattern emerging, law-enforcement officials say. Large groups of criminals are banding together to steal financial data from individuals, and then trade or sell that data on underground Internet sites.

One such case involves Shadowcrew, an online marketplace for stolen credit-card and debit-card information that U.S. agents shut down. The Web site, with some 4,000 members, served as the backbone of an extensive criminal organization that traded at least 1.5 million stolen credit-card numbers and caused total losses in excess of \$4 million, according to an indictment returned by a federal grand jury in Newark, N.J., in October.

The indictment names 19 individuals for their roles in running what the Department of Justice calls one of the largest online centers for trafficking stolen identity information, documents and banking details.

As public concern mounts about identity theft, police busts in the U.S., Europe and Latin America are shedding light on the increasing sophistication of the criminals behind such schemes. They are finding well-run, hierarchical organizations where members coordinate efforts via the Internet, often using aliases.

Once stolen, the information is advertised and sold on Web sites and Internet chat rooms specializing in the trafficking of such valuable data.

"They are run like businesses," says Larry Johnson, special agent in charge of the Secret Service's criminal investigative division, who helped coordinate the Shadowcrew investigation. Identity theft long predates the Web, but Mr. Johnson says the Internet helps large groups communicate much more efficiently and extend their geographical reach.

The rings often are international, including Shadowcrew, which had key members in several countries.

Identity theft cost consumers and their banks and credit-card companies about \$11.7 billion in losses for the 12 months through April 2004, estimates Gartner Inc., a Stamford, Conn., technology research firm. Gartner says it is difficult to know how much of that is attributable to crimes committed online rather than offline -- such as from stolen purses or wallets. But banks and law enforcement say that online identity theft is growing rapidly.

One widespread scam is known as phishing, which uses e-mails designed to look as if they are from a legitimate bank or retailer to trick consumers into entering credit card, banking or other sensitive information at fake Web sites. In a new twist, dubbed pharming, hackers manipulate the settings on a

computer so the user will be redirected to a counterfeit Web site when attempting to visit a legitimate Web site for service.

Major banks have been frequent targets of such attacks. A recent legitimate-looking e-mail to customers of [HSBC Holdings](#) PLC warned recipients that there had been several failed attempts to log onto their online accounts. The e-mail, bearing the HSBC logo, asked recipients to re-confirm their account information. It pointed customers to a Web site link beginning with the bank's real address, [www.hsbc.com](#), and warned that those who ignored the request would have their account suspended.

HSBC confirms the e-mail was fake but says it doesn't know how much money the scam may have swindled from customers. Customers who report that their accounts are missing money often don't know how their account numbers and passwords were stolen.

A large Brazilian gang allegedly swindled roughly \$66 million from online-banking customers using a computer virus attached to an e-mail that appeared to be from legitimate banks, says Paulo Quintiliano, head of the Brazilian federal police's cyber-crime division.

People who clicked on the link in the e-mail downloaded the virus onto their computers, which then stored the customer's bank details when they accessed their accounts online at legitimate banking sites. The computer code then sent the swiped account information and passwords to the hackers.

The gang then used the banking information to transfer money out of accounts, create fake bank cards and even set up shell companies through which they channeled the money, says Mr. Quintiliano.

Brazilian federal police have arrested and charged more than 100 members of the gang over the past 18 months, and a trial is under way.

The market for trading stolen information has grown more sophisticated in the past year, too, security experts say.

Originally, large volumes of credit-card or bank-account information were sold indiscriminately in bulk, says John Watters, chief executive of iDefense Inc., a Reston, Va., information-security consultant that monitors Web sites which market stolen data. Now, criminals are charging more if a card has a high credit limit or if valuable additional personal information -- such as a billing address and maiden name -- are included with the account number and PIN.

And information on overseas bank accounts is now commanding higher prices than data on accounts in the U.S., where security measures are perceived to be stiffer, adds Mr. Watters. An account number and PIN for a British bank account holding the equivalent of about \$3,000 can sell for \$200, which is double what a similar U.S. account fetches, he says. "It's the Nasdaq of the underground economy."

The operations often are international in scope. Police in the U.K. are pursuing an Eastern European gang that they believe stole millions of pounds from customers of British banks through fake e-mails, or phishing.

As part of that probe, the U.K.'s National Hi-Tech Crime Unit last June arrested two men, an American and a Scotsman, in the U.K. in connection with their alleged role as moderators of a Web site where stolen account and password information was traded. Police charged the men with conspiracy to defraud and money laundering.

The Shadowcrew Web-site case in New Jersey illustrates how criminal groups profit from stolen data. The indictment alleges that Shadowcrew members traded stolen personal data on a Web site called www.shadowcrew.com. Using online nicknames such as "Dirty Harry" and "NotoriousCarder," they bought and sold credit- and debit-card information, counterfeit drivers' licenses, passports and Social Security cards, the indictment alleges.

Among the leaders of the operation was 23-year-old Andrew Mantovani, of Scottsdale, Ariz., who along with other "administrators" directed the organization and handled day-to-day management decisions, the indictment alleges. "Reviewers" tested illicit merchandise before it could be sold. The information then was advertised and sold on shadowcrew.com, a password-protected site that was overseen by various "moderators."

According to the indictment, the organization reprimanded members who broke the rules. On one occasion, an administrator punished a member nicknamed "CCSupplier" for failing to pay other members, the indictment says. The penalty: The group posted CCSupplier's real name, address and phone numbers on the site.

What makes Shadowcrew noteworthy is "the level of sophistication and the level of organization of this online community," says assistant U.S. attorney Kevin O'Dowd in Newark.

The 62-count indictment carries five charges against Mr. Mantovani, including conspiracy, trafficking in stolen credit-card numbers and unlawful transfer of other personal information. Mr. Mantovani pleaded not guilty at his arraignment in February, according to his attorney, Pasquale Giannetta.

If convicted, Mr. Mantovani potentially faces more than 20 years in prison. A trial is scheduled for October.

The investigation also led to two other organizations -- called Carderplanet and Darkprofits -- that the Secret Service alleges operated similar Web sites to traffic in counterfeit credit cards and stolen personal data.

Authorities shut down those sites, but security experts expect the people behind them will just move their operations. "It's a cat and mouse game," says the Secret Service's Mr. Johnson.