

CITY BUSINESS



C R I M E

CREDIT RAPE

Thieves no longer are content to steal credit cards. Now, they want something far more valuable—credit reports.

In Sacramento and across the country, crooks are finding it a simple matter to obtain the confidential records of affluent individuals in order to pose as good credit risks and thus hoodwink banks and retailers out of loans for fancy cars, expensive jewelry, appliances, even real estate. Ultimately, the debts go unpaid, leaving victimized consumers with sullied credit reports that often prove impossible to clean up.

The act is known by various names: credit cloning is the most polite; credit rape is the most apt.

Whatever the name, experts say it is one of the most insidious financial crimes ever: Roughly three of every 200 credit applications processed nationwide are being submitted nowadays by impostors.

To commit credit rape, a perpetrator needs little more than a victim's name and social security number, says Glenn Johnson, a fraud investigator for GE Capital Corporation. Armed with this information, the scammer applies for a line of credit in his victim's name. Most of the personal financial data used to complete the application is guessed at, yet the ploy works because bankers and merchants typically ignore anything but computerized documentation supplied by credit-reporting bureaus.

"If the computer printout shows a good credit history, the application gets approved," says Johnson. "A lot of credit grantors don't see red flags when information on the application grossly mismatches the bureau printout. They're just too eager to get the application processed, approved and out of their hair."

Tighter scrutiny doesn't seem to help. Many thieves avoid discrepancies on their applications by obtaining copies of victims'

bureau-generated credit reports ahead of time. These printouts, Johnson indicates, often contain all the private information necessary for a credit cloner to compile a convincing application.

"The guy simply orders a copy of your report direct from the credit bureau," says Johnson. "He poses as you by substituting his own address—a mail drop, usually—in place of yours, which he lists as his recent former address. A lot of times that's enough to fool the bureau's computers.

"He may also be able to find reports discarded in trash bins behind finance companies, stores, car dealerships, or he can just purchase them from other crooks on the street."

Sale of illicitly procured personal data is a boom business locally, says a spokesman for the state attorney general's office. Just last year, for example, a Sacramento federal grand jury indicted two women who worked as clerks at a Northern California hospital for allegedly trafficking in confidential information stolen from patient files.

Only rarely, though, are credit scammers actually brought to justice. A common reason is that a great deal of time may elapse before victims stumble upon the damage to their credit ratings. "By then, the culprit has moved out of state," says Johnson. "Consumers don't catch on sooner because dunning notices from bill collectors are diverted to the mail drop."

The second reason is that state and federal laws recognize bankers and merchants, rather than consumers, as victims. "Most creditors who get burned don't press for prosecutions because it's too much trouble," says Johnson.

Consumers, left vulnerable and largely voiceless, are advised to protect themselves by periodically checking their credit reports for telltale activity and by requesting that the bureaus insert a statement instructing banks and merchants to call consumer-designated home and office telephone numbers in order to authenticate applications before granting credit.

—Rich Smith