

# Industry at Odds Over ID Theft Liability

By Joseph Menn  
Times Staff Writer

March 7, 2005

Heidi Anderson didn't know much about identity theft until her Christmas 2001 shopping trip to Victoria's Secret, where a cashier said her store card — which she had used only once before — was over its limit.

A check of her credit reports revealed the depth of Anderson's misfortune: Using her name and driver's license number, someone had opened 33 charge accounts and run up more than \$30,000 in debt.

Her finances wrecked for more than a year, Anderson couldn't use what had been a spotless credit record to qualify for a mortgage on the home she had just picked out with her fiance. "We lost our house," said Anderson, a university fundraiser in Southern California. "It has to be one of the worst experiences of my life."

Anderson is angry at the Redondo Beach woman who wronged her and was later convicted. But she also blames the financial industry, specifically the institutions that screen credit card applications, for making the thief's job so easy.

"They'll give anyone a credit card without checking," Anderson said. "Until we hold the companies accountable, nothing's going to be done."

It could be that financial institutions aren't hurrying to tighten standards because of a little-known fact: Retailers, not banks, generally absorb losses caused by identity thieves. That means the companies issuing credit cards have little incentive to scrutinize applications, critics contend.

"As long as they continue to make money by granting credit easily to thousands of people every day, we're still going to have the problems," said Beth Givens, director of the nonprofit Privacy Rights Clearinghouse, a consumer information and advocacy group.

Banks counter that they are as strict as they can reasonably be in screening applications. Moreover, they have successfully cut fraud by impostors opening new accounts, said Nessa Feddis, senior federal counsel of the American Bankers Assn.

"The numbers are way down. The banks are doing a much better job of verifying information," Feddis said, although she was unable to provide figures to support that contention.

Regardless of who is liable for losses, she added, banks want to keep a good reputation and keep merchants as their customers.

The prevalence of identity theft has been underscored in recent weeks by a pair of high-profile security breaches. Late last month a company that provides credit information to businesses, **ChoicePoint** Inc., said

records on 145,000 individuals were released to con artists posing as companies with legitimate use for the data. Shortly thereafter, **Bank of America** Corp. said it lost computer tapes containing personal information on federal employees who use 1.2 million bank-issued cards to pay for expenses.

Criminal investigators say the Internet has played a crucial role in the spread of identity theft, as thieves troll through massive databases and poorly secured websites. They also issue wave after wave of "phishing" attacks, in which consumers are lured by e-mail to spurious but official-looking websites and are asked to enter account numbers.

Identity theft annually victimizes 10 million Americans and costs \$50 billion, according to the Federal Trade Commission. But crimes are rarely prosecuted and sentences are generally light, said Judith Collins, a Michigan State University criminology professor who studies the subject.

Given the Privacy Rights Clearinghouse said lenders would extend credit based on little more than an address, Social Security number and birth date, all of which can be easily acquired by a thief.

Armed with new cards, the thieves often switch addresses, so that the victim never sees the bills that are piling up. Identity thieves then make purchases on the Internet, collecting and selling off the goods for cash. They also can try to tap into other accounts held by the victim. If they succeed in transferring money, the consumer often can't get it back.

Merchants usually end up holding the bag.

Most feel that they have to honor major credit cards, which gives the issuers leverage in negotiating contracts with them. Under those contracts, the merchants are almost always responsible for losses in transactions conducted over the Internet, over the phone or through the mail.

In the face-to-face fraud that occurs inside physical stores, the issuing banks are theoretically responsible. But they can demand months-old receipts and other information that make it hard for the store to prove it was blameless.

"It usually winds up with the merchant," said Visa USA Vice President Rhonda Bentz.

The retail industry isn't happy about the situation, which is getting worse as electronic deals become more common. "Long term, we'd like to see a sharing in responsibility for those fraudulent orders," said Julie Ferguson, co-chair of the Merchant Risk Council, which advises online vendors on security.

That hasn't happened so far because of the balance of power in commerce and in Washington, where financial institutions spend more than triple the amount on lobbying that retailers do, according to the nonprofit Center for Responsive Politics. Retailers have nowhere near the same clout and "they're just not organized," said Avivah Litan, a Gartner Inc. analyst who has followed information security practices for years.

Banking industry officials deny that the lack of financial risk makes them less than vigilant about preventing identity thieves from opening fraudulent accounts.

For example, Visa's Bentz said, banks run credit applications against a database that includes names, addresses and phone numbers. If everything doesn't match, "a flag goes to the issuing bank, and they make a determination about whether to extend credit."

Bentz said such procedures had made "new-account" fraud, which is typically the most expensive and exasperating for victims, a rarity. But as recently as September 2003, the FTC estimated that new-account fraud made up about a third of all identity theft.

Banks also disagree with critics who say they should do more to alert consumers when security breaches result in leaks of confidential information that could make them vulnerable to identity theft.

The Secret Service notifies the credit card associations when it finds a new trove of personal information getting sold or offered free on the Internet. But Visa and MasterCard leave it up to the banks that issued those cards to warn consumers, and most choose not to — in part because it costs \$25 to issue a new card, Bentz said.

"Just because an account number has been taken doesn't mean there's any fraud on it," she said.

The card associations and banks also oppose creating a national version of California's law requiring broad disclosure after security breaches. John Hall, a spokesman for the American Bankers Assn., said mandated disclosure could create "a cry-wolf mentality."

Lax security by merchants is another cause of fraud, according to privacy advocates and law enforcement. Many stores fail to encrypt the information they keep on their customers or don't keep their computers secured.

And when notified that they have been hacked, most retailers never warn their customers.

Notifications under the California law, have been issued at least 45 times since it took effect in July 2003, said Joanne McNabb, who heads California's Office of Privacy Protection.

Elsewhere in the U.S., such warnings are rare, experts said.

Merchants are "very cautious, because it affects their bottom line. They don't want any publicity," said Larry Johnson, special agent in charge of the Secret Service's criminal investigations unit.

That bothers people like Dan Clements, whose company Card Cops.com scours the Net for credit card trafficking and notifies stores that have been hacked.

"The government bungles around and never really catches the ID thieves or notifies the consumer," Clements said. "It's on no one's agenda."

---

If you want other stories on this topic, search the Archives at [latimes.com/archives](http://latimes.com/archives).

**TMSReprints**

Article licensing and reprint options

Copyright 2005 Los Angeles Times