



Money

Search MSN

Money: [Help](#)

Financial Tools

[Track your bills](#)

Resources

[Decision Centers](#)

[Home Buying Guide](#)

[Home Financing](#)

[Your Credit](#)

[Rating](#)

[Financial Privacy](#)

[Better Banking](#)

[Credit Card Smarts](#)

[Bankruptcy Guide](#)

[Commentary Index](#)

Related Links

[Manage Debt](#)

[More on Budgeting](#)



Liz Pulliam Weston

[Print-friendly version](#)
[Send this to a friend](#)



The Basics

Banks hang fraud victims high and dry

advertisement

If a thief uses a stolen ATM card or checks to pilfer your accounts, you may not get much sympathy from your bank -- or any of your money back.

By [Liz Pulliam Weston](#)

Lesa Henderson of San Diego was shocked when her husband's paycheck suddenly disappeared from their checking account. But their troubles were just beginning.

An acquaintance who stole both Henderson's debit card and checks from her checkbook had drained every penny from the account. The Henderson's bank initially restored some of the lost money, which the thief promptly stole. The bank then decided the thefts were Lesa's fault because she had allowed the thief into her home. The bank demanded the Hendersons pay back the restored funds, plus all the fees from bounced checks. Furthermore, it refused to let the Hendersons close the compromised account because it was

[Analyze your spending](#)

[Personal finance bookshelf](#)

[Track your financial affairs here](#)

[Shop for money management resources](#)

[Do your taxes online](#)

Find It!

[Article Index](#)

[Fast Answers](#)

[Tools Index](#)

[Site Map](#)



Recent articles by Liz Pulliam Weston:

- [Feds target Grandma's Medicaid](#), 1/22/2006
 - [Uncle Sam cracks the whip on students](#), 1/18/2006
 - [How to blitz your holiday debts](#), 1/15/2006
- [More...](#)

overdrawn.

The thief's transactions kept getting processed, and the Hendersons kept getting dunned for returned-check fees -- a nightmare that went on for weeks.

Find a loan that's right for you at the **[Loan Center](#)**

"I was in tears. I just couldn't take another minute," Lesa said. "I couldn't fix this."

The Hendersons finally enlisted the help of San Diego's [Identity Theft Resource Center](#), which negotiated with the bank to allow them to close the account. The center is working on getting at least some of the Hendersons' money restored, but stay-at-home mother Lesa worries she'll have to go back to work to cover the "thousands of dollars" the bank still says she owes.

Check fraud 'is so much easier'

The Hendersons aren't an anomaly. Even as credit card fraud is waning, checking-account fraud appears to be rising, and some banks are playing hardball to try to stem their losses.

[Related news and commentary on MSN Money](#)



- [Your paper check is a thief's best friend](#)
 - [8 signs you may know an ID thief](#)
 - [Lost your wallet? Act fast](#)
 - [A fresh start on credit – without bankruptcy](#)
-

Gartner Research estimates 3 million Americans were victimized by ATM and debit card fraud in the 12 months ending May 2005. The technology research company estimated the total losses at \$2.75 billion for the year, or \$900 per customer, which it believes is a sharp escalation from previous years.

The American Bankers Association, which represents the industry, says the Gartner numbers are overblown. But the association's most recent debit fraud numbers are from 2003, when it says banks lost \$145 million to PIN- and signature-based debit-card fraud.

Losses from credit card fraud, meanwhile, have shrunk from \$1.80 per \$1,000 charged in the mid-1990s to 50 cents for the same \$1,000 today.

The bad guys have figured it out: "Checking account fraud is so much easier" than credit card fraud, said Ted Crooks, a fraud expert with Fair Isaac Corp.

Here's why:

Banks typically don't use software to spot suspicious trends. Most credit card issuers use programs, like Fair Isaac's Falcon software, that can flag transactions that don't fit the user's typical pattern. But few banks employ such programs to monitor checking accounts, Crooks said, although more are expressing interest as losses increase.

Banks often don't verify a card is real. The magnetic strip on the back of your debit or ATM card includes security codes that confirm the plastic was issued by your bank. But Gartner estimates as many as half of banks don't check those codes before authorizing transactions. A counterfeiter who dummies up a card using your number is thus very likely to be able to use it for fraudulent transactions.

Banks can blame the victim. Federal law prohibits credit card companies from holding customers responsible for unauthorized charges once the customers have reported the loss or theft of their card, and most issuers waive the \$50 liability they could charge for fraudulent transactions.

The rules are somewhat different for bank accounts. When a fraudulent debit charge or automatic payment is reported, a section of federal law known as Regulation E requires banks to investigate within 10 days. But banks can extend that period to 45 days if they credit the

disputed amount or \$2,500, whichever is less, to the customer's account. (Paper checks offer even less protection, as I discussed in "[Your paper check is a thief's best friend.](#)")

But a bank can decide there was no fraud, experts say, and take the money back as long as it provides a written explanation to the customer. That's what happened to the Hendersons and to Los Angeles Times columnist Steve Lopez, who recently wrote about his bank snatching back the \$2,020.50 it had restored to his account after a theft.

Banks say 'victims' work the system

You may be particularly vulnerable if the thief is using your personal identification number for transactions. Bank investigators may decide that if someone stole your PIN, you must be in cahoots or at least have given tacit permission to be ripped off.

The banks aren't always wrong, of course. "There are a lot of flaky people out there," said Crooks, adding that some "know in the back of their mind that it was Junior" who swiped their account information.

Others knowingly manipulate the system, said American Bankers Association spokesman John Hall. In fact, he said, the majority of people reporting bank fraud aren't victims at all.

"It happens a lot," Hall said. "People know the law and take advantage of Regulation E."

Ways thieves get to your accounts

But there are plenty of ways thieves can victimize unsuspecting consumers and even snatch their PINs, including:

- **Dummy or compromised ATMs.**
Resourceful thieves can set out phony ATMs or place devices known as "skimmers" on a legitimate machine. The skimmers fit over the intake slot and copy account information off the magnetic strip. Tiny cameras pointed at the keypad record your PIN.
- **Phishing.** An authentic-looking e-mail warns of trouble in your account and asks you to "confirm" or "re-enter" your card number and PIN. [The Anti-Phishing Working Group](#), a global industry and law-enforcement coalition targeting this fraud, said it received nearly 17,000 reports of phishing in November 2005, nearly twice the level of a year earlier.
- **Malware.** An infected e-mail or Web site installs a keystroke logging program on your computer, which can capture and transmit your codes to a thief. Again, the reported incidence of these programs and sites has spiked in the last year, according to the group.
- **Crooked insiders.** Employees at the bank

or at retail locations may have access to the data collected off your card.

Or thieves may get it by brute force.

"I could use my elbow to break open the front (of a gas pump) and pull out the hard drive," said Jay Foley, co-founder of the Identity Theft Resource Center. Chances are the data on that hard drive aren't encrypted, "so I've got the last 24 hours' worth of card numbers and PINs."

Page 1 of 2 Story continues on [next page](#) 

MSN Money's editorial goal is to provide a forum for personal finance and investment ideas. Our articles, columns, message board posts and other features should not be construed as investment advice, nor does their appearance imply an endorsement by Microsoft of any specific security or trading strategy. An investor's best course of action must be based on individual circumstances.