




September 22, 2007

In Data Leaks, Culprits Often Are Mom, Pop

**Credit-Card Industry
Tries to Add Safeguards;
Honest Errors Common**

By **ROBIN SIDEL**
September 22, 2007

DOW JONES REPRINTS

 This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit: www.djreprints.com.

- [See a sample reprint in PDF format.](#)
- [Order a reprint of this article now.](#)

As more people use plastic to pay for smaller purchases, countless mom-and-pop shops and restaurateurs are running afoul of rules designed to protect people's personal data.

Smaller shops have proven ill-prepared for the complexities of safeguarding credit-card information. Since 2005, more than 80% of the instances of unauthorized access to card data have involved small merchants, according to Visa USA Inc., the largest payment-card network. These businesses account for 85% of the seven million locations nationwide that accept plastic, according to Visa.

RESTAURANT VIOLATION

- **The Situation:** Many smaller restaurants aren't protecting customers' credit-card data.
- **Background:** These smaller businesses apparently don't update software enough and keep on top of the new rules designed to keep data safe.
- **Safer With a Giant?** Most large retailers upgrade their computer systems regularly.

All merchants are supposed to follow card-industry rules to prevent account information from falling into the wrong hands. But the industry has generally focused on larger retailers. For instance, starting Oct. 1, big merchants face fines of \$25,000 a month for noncompliance.

Many small merchants aren't even aware that the rules exist. These store owners "are provided with no information and, sometimes, with erroneous information," says Anita Boomstein, a lawyer at Hughes Hubbard & Reed LLP who represents small merchants.

Among them: Roger Rehmke, owner of Lodi Beer, a microbrewery and restaurant in Lodi, Calif. In January, Lodi Beer was identified as a common point of purchase among some cardholders whose accounts had been compromised, exposing them to potential fraud. It was then that Mr. Rehmke discovered his computer system had stored account data on 11,728 customers -- a violation of card-industry rules, which prohibit retailers from retaining some of this information on their local computers.

He says he had no idea about the violation. "All someone had to do is tell us 'you can't do that,' " he says. "We would have changed it."

The magnetic strips on the backs of credit cards contain cardholders' names and account numbers,

expiration dates, and security codes used to authorize certain purchases. When a consumer uses a card, the merchant's computer captures that information.

Yet storing that data puts cardholders at risk: Computer hackers who get their hands on the information can use it to make fraudulent purchases.

Consumers typically aren't liable for fraudulent purchases on their credit cards, but the theft of card data can still create big headaches, particularly if the information is used to create a fake identity. Industry experts recommend that cardholders scour their account statements regularly and report irregularities as soon as they are spotted.

U.S. financial institutions that issue credit cards incurred a record \$1.24 billion of losses from fraud last year, up 9.3% from 2005, according to Nilson Report, an industry newsletter based in Carpinteria, Calif. Most credit-card fraud, by dollar volume, tied to merchants occurs because hackers broke into the networks of big retailers.

There are no nationwide laws against storing card data. Indeed, the card industry lets merchants store some data, but its rules prohibit storing the most-sensitive information, such as the special three-digit or four-digit security codes that sometimes are on the back of cards.

Despite those rules, a recent survey of more than 600 businesses with fewer than 250 employees found that 52% of them were storing sensitive customer information on their computers, according to Visa and the National Federation of Independent Business, a trade group.

Where's the Security?

"You wonder how they got hacked, and then you find that there is no security on their system whatsoever," says Bryan Sartin, vice president of Cybertrust Inc., a data-security firm hired by Mr. Rehmke.

Until recently, card-industry efforts to educate small merchants were haphazard. On July 31, Visa International Inc.'s Visa USA began requiring about 270 card processors to submit plans for getting small businesses to comply with the rules. Visa and MasterCard Inc. are working with small-business organizations and data-security firms to spread the word.

In February, local police told Ohio restaurant owners Richard and Paulette Schnipke that some of their customers' cards had been compromised. The Schnipkes say they were surprised to discover that their computer system was storing card information.

"When we purchased the computer system and saw that the [account] numbers weren't showing up on the customer receipt, I just assumed we were compliant," says Mrs. Schnipke, whose family owns Red Pig Inn restaurants in the towns of Findlay and Ottawa.

Attentive Wife

Lodi Beer's problems started when Mr. Rehmke's wife, Sam, who handles the books, noticed that the restaurant's checking account wasn't reflecting credit-card deposits. After several phone calls, the couple learned that patrons had experienced fraud on their cards.

Although there was no conclusive evidence that hackers had broken into Lodi Beer's system, its

card processor, Abanco International LLC, decided to freeze its account, which caused the Rehmkes to bounce several checks. Credit and debit cards account for about 70% of their restaurant's sales.

An audit of Lodi Beer's computer system revealed that it had been storing cardholders' data, including account numbers, for three years. The couple has since spent thousands of dollars to upgrade the computer system.

Visa and MasterCard fined Abanco \$27,000 for Lodi Beer's noncompliance. Abanco passed on the fine to the Rehmkes -- the equivalent of five days of sales.

Michael Rosenbloom, a lawyer for Abanco, says the company didn't typically provide recommendations to its customers about data security. Card-processing contracts, he explains, call for merchants to follow card-industry rules. Still, he concedes that it's "a little bit far-fetched" to think that merchants will know that they must "actually go on the Visa Web site and review the rules."

In April, Abanco sold its merchant-processing business to New York-based Cynergy Data.

The biggest merchants face the toughest requirements because they are most often targeted by hackers. Yet only 39% of the nation's largest 327 merchants have proven that they are in compliance, according to Visa.

Since October, Visa has levied \$3.3 million in fines against processing companies whose large-merchant customers aren't following the rules. MasterCard doesn't disclose fine totals.

Out-of-Date Software

While most large retailers upgrade their computer systems regularly, using one of the dozens of versions of payment software that has Visa's stamp of approval, that isn't the case for small merchants. Many of them grow comfortable with one type of software.

In May, Minnesota passed the Plastic Card Security Act, which prohibits companies doing business in the state from storing sensitive card information. The law, which took effect in August, makes violators liable for costs associated with computer breaches or fraud.

Brad Friedlander, who owns two Cleveland restaurants, says he has paid about \$50,000 for fines and computer upgrades after being alerted by law-enforcement officials of a possible security breach.

"I had passwords and a firewall," says Mr. Friedlander. "I thought I was doing everything I was supposed to do. I'm not a computer person."

Write to Robin Sidel at robin.sidel@wsj.com¹

URL for this article:

<http://online.wsj.com/article/SB119042666704635941.html>

Hyperlinks in this Article:

(1) <mailto:robin.sidel@wsj.com>

Copyright 2008 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our [Subscriber Agreement](#) and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com.

RELATED ARTICLES FROM ACROSS THE WEB

Related Content may require a subscription | [Subscribe Now -- Get 2 Weeks FREE](#)

Related Articles from WSJ.com

- [Citigroup Debit Cards for China](#) Jul. 17, 2008
- [Visa Stops Requiring PIN For Debit-Card Purchases](#) Jul. 02, 2008
- [Nobody's Snapping Up GE's Plastic](#) Jun. 26, 2008
- [Mossberg's Mailbox](#) Jun. 23, 2008

More related content Powered by *Sphere* 