Arizona Daily Star®
www.dailystar.com® www.azstarnet.com®

Published: 04.28.2005

Thieves get buyer info stored when card is used

By David Bank
THE WALL STREET JOURNAL

Credit report

- Consumers can request a free credit report once a year.
- www.annualcreditreport.com
- 1-877-322-8228

There's a common thread to some of the recent security breaches at retailers that exposed sensitive financial details of hundreds of thousands of customers: software that retailers say improperly stored credit-card data.

The computerized systems that manage much of U.S. commerce are supposed to purge most credit-card information - including a secret three-digit code that can enable criminals to counterfeit cards - after each transaction. But merchants, banks and credit-card associations say many widely used retail-software packages often retain this information - creating an alluring target for hackers.

The recently revealed security breach at Polo Ralph Lauren Corp. is a case in point. Banking giant HSBC PLC notified the clothier last fall that credit-card data from some of its customers may have been compromised.

A Polo spokeswoman said an investigation found that the software Polo has used at checkout counters in more than 180 stores improperly retained the sensitive card details. Polo scrambled to purge the data from its systems.

Hundreds of merchants are now conducting similar purges. In at least one case, security experts say, hackers hit a half-dozen merchants that use similar software after figuring out how to tap into these three-digit codes.

The sensitive information encoded in the magnetic stripe on credit cards "was out there more than we thought," says John Shaughnessy, senior vice president for risk management at Visa USA. These secret codes are "jewels" for thieves, he says. "The fact that it's stored anywhere is troublesome."

The three-digit number on the magnetic stripe - which is different from the visible verification codes found on the backs of most credit cards - is particularly sensitive because it is necessary for creating counterfeit cards.

The secret code can be used to produce a card in which the visible name on the card's front need not match the account information on the magnetic stripe. That could allow fraudsters to present a driver's license or other identification to "validate" a fake card.

But the account number on the stripe isn't that of the person who's name is on the front of the card. Many times the fraudulent purchase wouldn't even be known or reported until the victim of the card theft sees his or her monthly statement.

As concerns mount over these breaches of the magnetic-stripe data, merchants are starting to point fingers at their technology suppliers. BJ's Wholesale Club Inc. has gone further, suing IBM to compensate it for losses stemming from a credit-card breach.

In the suit filed last fall, BJ's says that, unknown to its executives, IBM's software stored customers' credit-card information on computer logs. BJ's faces suits by a number of banks and credit unions for damages after hackers stole as many as 40,000 credit-card numbers of BJ's customers. BJ's has set aside $16 million to cover its potential losses.

IBM says in legal filings that there's no proof the card numbers were taken from BJ's computers, and that its contract with BJ's specifies that it isn't responsible for damages from a security breach.

Visa, MasterCard and other credit-card associations bar storing information from a card's magnetic stripe after a transaction is completed. Visa's guidelines provide for penalties of as much as $500,000 for violations.

In the wake of the BJ's breach, Visa last summer called a meeting of two dozen software suppliers to stress the importance of cleaning up their systems. Since February, Visa has been checking software to make sure it doesn't retain sensitive information. So far, it has approved only seven systems, but not IBM's.

The rush by retailers to purge credit-card data is part of a larger reversal in what had been a trend toward capturing ever-greater quantities of customer information for marketing purposes.

"Ten years ago, it was, 'Store all the data you can,' " says Chris Noell, vice president of Solutionary Inc., which audits merchants' security systems. "Now the thinking is, 'Some of this exposes you to liability. Don't keep it.' "