

 [Print this article](#)

[Close This Window](#)

TJX card problem flags retail identify theft risk

Fri Mar 30, 2007 8:32 PM ET

By Brad Dorfman

CHICAGO (Reuters) - Consumers who want to be sure about protecting their personal data and preventing identity theft might need to pay solely with cash, shun retailer loyalty programs and only make returns when they have a receipt.

Otherwise, they could be turning over data to a retailer vulnerable to hackers hunting for credit card information, social security numbers and anything else they can use to commit fraud, computer security and financial experts said on Friday.

"The retail sector has some unique vulnerabilities from the older technologies they use, often from legacy systems," said Tom Arnold, partner at PSC, a San Jose, California-based data security and compliance consulting firm. "Adopting more up-to-date security standards has been a slow process."

Retailers are, and have been, spending millions of dollars to upgrade their computer systems to prevent theft, said Mallory Duncan, general counsel for the National Retail Federation (NRF), a retail industry trade group.

Duncan said the percentage of all security breaches at retailers are in the single digits, but such breaches get more attention because the companies are usually so well known.

"Retailers are very concerned about this, because, just like anyone else, they don't like being burgled," Duncan said. "Very sophisticated criminals are hacking into very secure systems and making off with our corporate information."

Retailer TJX Cos. Inc. said on Thursday information from 45.7 million credit and debit cards was stolen in a computer security breach over 18 months through mid-January.

Other information, including names, addresses and personal ID numbers for about 451,000 people who returned merchandise without a receipt, was also stolen, the operator of the T.J. Maxx and Marshall's chains said in a regulatory filing.

HELP WANTED: ENFORCEMENT

Retailers constantly ask buyers for personal information in order to find out more about spending habits, demographics and which promotions work on what types of customers.

That data, along with credit and debit card information, become a treasure trove for thieves who are constantly assaulting computer systems, looking for a way to get at it.

And unlike a person caught trying to rob a bank, hackers generally are not punished for failed attempts, so they keep trying again, said Terrence DeFranco, chief executive of Edentify Inc., a computer security company.

"The thing that empowers them is that even if intrusion is detected and prevented, you don't get penalized for the attempt," DeFranco said. "As a perpetrator, I have the benefit of trial and error."

NRF's Duncan said the retail industry wants law enforcement to be more active in pursuing hackers who do break in.

"Ideally, we want to throw the book at hackers," Duncan said.

To DeFranco, there are two types of people: those who have had their data stolen and those that will.

"The only way to be perfectly safe is to never give your information out or never have anyone else give your information out from the time you are born until the time you die," DeFranco said.

But being more realistic, experts suggest several steps, including monitoring credit reports, card and bank statements to check for unauthorized transactions and shredding documents that contain personal and financial information.

DeFranco even opens all the junk mail he gets to try to determine where the solicitor got his information.

"Retailers need to become more secure," said Christine Pratt, research director for consumer banking and credit at Financial Insights, a research advisory firm. "This is a spot where retailers in particular fell down."

(Additional reporting by Jonathan Stempel in New York)