

Security of wireless networks often leaves retailers, credit card firms at risk

Theft, breaches likely to increase in tough times

By Wailin Wong | Tribune reporter
March 6, 2009



Motorola's Richard Rushing walks Michigan Avenue on Feb. 2, checking the security of wireless access points at surrounding stores. (Tribune photo by Nancy Stone / February 2, 2009)

Richard Rushing has walked the Champs-Élysées in Paris and strolled an underground mall in Seoul. But he's not a shopper. He's a wireless security expert who scans the airwaves in busy retail areas to study how stores are protecting your data.

"Retailers have always taken security very seriously," said Rushing, senior director of information security for mobile devices at [Motorola Inc.](#), noting the common use of security cameras and guards.

"But they're not looking at the airwaves to see what's leaking out of their stores wirelessly. You don't need the merchandise if you can steal a credit card number and buy a gift card," Rushing said.

Most consumers don't think about what happens to their credit card information when they swipe their plastic at the cash register. The reality is that large retailers have wireless networks that connect cash registers, bar code scanners and store computers. Those networks can be vulnerable to breaches by hackers or thieves.

In some high-profile cases, thieves didn't pluck one card number but tens of millions.

In 2007, discount retailer [TJX Cos.](#) said a computer breach exposed 45.7 million credit and debit cards to account information theft. The group accused of stealing the TJX data was believed to have hacked into several stores' weakly encrypted wireless networks. Last year, supermarket company Hannaford Bros. reported a data breach, saying customer accounts at stores in the Northeast and [Florida](#) were compromised.

Stan Schatt, a vice president at ABI Research, said some retailers are bracing for an uptick in crime because of the economic downturn, whether it's increased shoplifting or employee theft. "What I'm hearing is that some retailers are cutting back in opening new stores and instead are plowing some money into security."

His research shows 77 percent of retailers with 500 or more employees use wireless networks.

"Retailers work on very thin margins, and even a small increase in theft can wipe out their profit margins completely," Schatt said.

In February, Rushing conducted a "war walk" simulation along the [Magnificent Mile](#), ambling up the sidewalk with a laptop that had an antenna affixed to the side. Proprietary software collected information about active wireless devices and the level of encryption for those networks.

In Rushing's brief circuit, which took him four blocks on Michigan Avenue before he turned around, he passed about 80 stores and detected 140 "access points," or devices that connect wireless gadgets such as computers to the network. Close to one-third of the access points counted during his walk used an older encryption standard called WEP that can be broken in 90 seconds, he said.

The retail industry shares responsibility for security with others in the payment chain, including credit card processors.

In January, payment processor [Heartland Payment Systems](#) announced it had found malicious software in its systems that potentially put at risk customer information associated with the 100 million card transactions it handles each month.

Dave Taylor, founder of the PCI Knowledge Base, which helps members of the payment card industry meet security standards, said the financial liability in data breaches makes the issue of security a hot potato. TJX had to set aside \$24 million in a settlement with MasterCard Inc.

"TJX and Hannaford had retailers running around like crazy," Taylor said. "Since the big breaches with payment providers, you have retailers pointing their fingers."

Taylor and Rushing emphasized that protecting wireless networks involves more than proper setup and encryption.

Retailers must be careful about employee access and keeping track of portable devices shared among workers.

In many cases of fraud, "the wireless is just the getaway car," Rushing said.

wawong@tribune.com