



**November 15, 2007**

## **WSJ: Retailers' Data Systems Vulnerable To Hackers - Survey**

By Joseph Pereira  
Of The Wall Street Journal

BOSTON (Dow Jones)--A number of retail stores may be vulnerable to hacker attacks this holiday season, according to a recent study by a wireless security firm.

AirDefense Inc. on Thursday is to release the results of a six-week undercover investigation into the electronic data security systems at more than 3,000 stores nationwide and abroad.

"I don't want to scare myself and not shop this Christmas," Richard Rushing, the company's chief security officer and project organizer, told The Wall Street Journal. "Knowing what we know now, I'm trying really hard not to do that."

Rushing, who concluded his study earlier this month, said computer thieves - if they wished to do so today - could with little difficulty break into 42% of the stores monitored by AirDefense.

Among the 3,000 stores surveyed, AirDefense found nearly 5,000 access points through which electronic thieves could enter the computer networks of retailers. Nearly 30% of retailers either used either no encryptions or easily crackable Wired Equivalent Privacy protocol, or WEP.

The survey also noted that 84% of the more than 2,500 wireless devices used by retailers, from cash registers and laptops to barcode scanners, could be compromised because they were outdated or misconfigured.

About 70% of the retailers surveyed were using stronger and more up-to-date encryption protocols. But some of them hadn't switched off their WEP systems, leaving their access points still exposed to outside intrusions.

Rushing said the AirDefense survey included 51 of the 100 largest retail chains in the U.S.

For his investigation, Rushing traveled to some of the busiest shopping areas in the country, including Rodeo Drive in Beverly Hills; Madison and Fifth avenues in New York; Michigan Avenue in Chicago and Union and Market streets in San Francisco. Research overseas was conducted at the Champs Elysees in Paris and Piccadilly Circus in London.

For his study, Rushing said his firm used typical hacking equipment, including a signal-intercepting radio wave antenna, deciphering software and other descrambling devices. The equipment enabled Rushing to see transactional data of customers along with user names and passwords of store employees. Rushing conducted part of his survey by walking through stores with his equipment hidden in a backpack.

The survey was undertaken without the knowledge of the retailers, Rushing said. But he added that what he did isn't considered illegal because he did not download any of the data.

AirDefense declined to name any of the retailers it monitored, in order to keep hackers from acting on its information.

Such a survey could be beneficial to AirDefense, an Atlanta-based concern that makes intrusion prevention security systems. Its findings are being disclosed just before the start of this year's holiday shopping season.

"Retailers around the country are leaving the `proverbial' barn door open for potential problems," said Rushing. Hackers seeking to steal credit card data aren't the only ones that could cause havoc. A retailer could potentially cripple a rival's network by gaining access through one of these points.

"What's called `Black Friday,'" Rushing said, referring to the the frenzied shopping day following Thanksgiving, "could be turned into a real black Friday."