



Banks Must Share Responsibility for Retailer Breach

By Avivah Litan

On January 17, 2006, the TJX Companies, parent company of a large number of retailers, reported it had discovered an “unauthorized intrusion into its computer systems that process and store information related to customer transactions” and determined that some customer information was stolen. TJX said the extent of the theft remains unknown, but many banks have already reported substantial fraud losses linked to the breach.

This breach appears to be a well-targeted attack. Law enforcement officials tell research firm Gartner Inc. that sophisticated cyber thieves are assembling portfolios on consumers by piecing together data stolen through such methods as phishing, keystroke logging, bank and brokerage account takeover and hacks into retailer systems. Attacks against large retailer systems are not going away—if anything, they are escalating as cyber thieves set their sights on their large data stores.

Retail payment systems were not designed with security in mind, and hackers are finding the weakest links—especially among retailers that have the most sensitive data stored. U.S. card issuers that Gartner has spoken with in recent months say counterfeit fraud is at an all-time high, and the card brands (e.g. Visa, MasterCard) are cracking down on retailer storage of magnetic-stripe card data whose theft enables counterfeit operations. The card companies are making progress on this limited front, but it’s an uphill battle and there are many more fronts on which to fight.

Securing thousands of complex and diffuse retailer systems is an overwhelming task, and even if they are secured, new vulnerabilities will inevitably emerge as systems continually change

The opinions expressed are those of the author(s) and do not represent the views of Transaction Trends, the Electronic Transactions Association, the association's board of directors, staff or members. We welcome reader articles and letters to the editor that express a differing point of view. Inclusion of responses in future issues of the magazine will be at the discretion of the publisher. Transaction Trends reserves the right to edit all submissions. Responses must include the name, address and daytime telephone number of the author. Submit to:

Transaction Trends Opinion
Electronic Transactions Association
1101 16th Street NW Suite 402
Washington, DC 20036
Fax: 202-828-2639
E-mail: opinion@electran.org

over time. The card industry must face the fact that it cannot rely solely on retailers to strengthen the security of the U.S. retail payment system. U.S. card issuers should implement stronger cardholder authentication, as they have in other parts of the world, while retailers continue to upgrade their own security infrastructure.

By instituting stronger cardholder authentication, card issuers would render stolen electronic card information useless. Some technologies already on the market, such as dynamic one-time passwords (OTPs) built into cards, would require minimal changes to the payment systems infrastructure because it’s already set up to process PINs, albeit static ones.

The only way stolen OTP-protected card information can be used is if the thief steals the card itself. Stronger authentication methods, such as those enabled by the Europay MasterCard Visa integrated chip card standard and PIN standard, cost much more to implement but provide more robust security because the thieves must have both physical possession of the card and knowledge of the user’s PIN.

Banks have much to lose with counterfeit fraud because they must reimburse consumers whose card data was stolen, and consumer confidence in the card-payment systems will erode as more breaches occur. The card industry is pressuring retailers to comply with the Payment Card Industry (PCI) data security standard promulgated by Visa and MasterCard. However, progress on that front is slow. As of October 2006, only one-third (about 100) of the largest (Level 1) retailers were compliant with the PCI standard.

Indeed, retailer payment systems were put in place many years before the emergence of sophisticated cyber attacks. The banking industry has enjoyed healthy revenues from the interchange fees retailers pay, and fees have been set higher to cover issuer fraud losses. In the past, card issuers consciously opted for high convenience rather than high security. That formula used to work well, but that was before the emergence of highly skilled criminals and widespread business use of the Internet. It’s time to shift the balance and tilt it more toward security. In the end, more fraud will mean higher prices for consumers, no matter how costs are shared across retailers and banks.

Simply stated, it’s unrealistic for the card industry to expect the approximately 5 million U.S. retailers that accept credit cards to become security experts and change their systems and/or processes to fix security holes. Although sensitive retailer data should of course be secured, banks also must own up to the problem. It’s a collective problem that demands a collective solution. **TT**

Avivah Litan is vice president and distinguished analyst with research firm Gartner Inc.