CHAIN STORE AGE®
THE NEWSMAGAZINE FOR RETAIL EXECUTIVES
SEPTEMBER 2007 www.chainstoreage.com A LEBHAR-FRIEDMAN® PUBLICATION

Shakin' Up Compliance

Steak n Shake meets challenges of PCI-regulated credit-card transactions

By Connie Robbins Gentry

Before a restaurant achieves level 1 status by the Payment Card Industry (PCI) standards, it could be scooping ice cream, swiping credit cards and worrying about nothing more than an annual self-assessment questionnaire and a relatively low-key quarterly audit by a PCI vendor. Granted, the restaurant may be swiping 5 or 6 million credit cards annually—but merchants such as Steak n Shake like it when ice-cream sales are hot.

However, swipe that 6,000,001st credit-card payment and pressures heat up. The convenience of credit-card payments can lead to chaos when a merchant crosses the threshold that requires compliance to more stringent PCI standards.

In August 2006, Indianapolis-based Steak n Shake was notified that it had achieved PCI's "level 1" status, meaning it was processing more than 6 million transactions annually. At this level, the chain's corporate network and its 490 restaurant locations would have to comply with the industry's most stringent electronic security standards, enforced through an annual onsite security audit as well as a quarterly network-security scan.

Steak n Shake has only been accepting credit-card transactions for a few years, but the volume of plastic transactions has grown exponentially—driven by consumer preferences for the convenience of credit as well as Steak n Shake's continued growth of 25 to 30 new store openings per year.

"I'd say the vast majority of our transactions have swung from cash to credit," acknowledged Sean Smith, director of strategic technology services for Steak n Shake, which had sales of $638.8 million in 2006. "In the last year, we had in the neighborhood of 14 to 16 million credit-card transactions."

"When we got the notification last August, we immediately looked at the requirements and performed onsite assessments of potential gaps and vulnerabilities in our processes and systems," said Smith. "Parallel to that assessment, we rolled out a PCI-certified credit-card service from Xpient [Charlotte, N.C.] to make sure our credit-card applications were up to par."

> "The vast majority of our transactions have swung from cash to credit."
>
> —Sean Smith, director of strategic technology services, Steak n Shake

After identifying areas for remediation, a complete strategy was developed around the areas of cash management, anti-virus and spyware solutions, and the company's perimeter network security. The strategy also identified needed changes in policies and procedures, including the training and education for management at the store level.

"As far as the perimeter security was concerned, we replaced firewalls and [upgraded] our VPN [virtual private network] technology," continued Smith. "We've also implemented intrusion protection and detection [software]."

The upgraded system provides triggers and alerts on any interesting traffic or anomalies. Steak n Shake is rolling out a patch-management system from Lindon, Utah-based Altiris as well as the McAfee total-protection suite.

"To get a complete view of our environment, with both external and internal scans, we are implementing a Qualys platform," Smith explained.

Qualys, based in Redwood Shores, Calif., provides a software-as-a-service platform that secures company networks and conducts automated security audits to ensure compliance with policies and regulations.

"Through the external scan, which basically entails the perimeter of our organization—such as active postings that anyone could see from the Internet—Qualys identifies and remediates any vulnerabilities," noted Smith.

Credit-card data obtained at the point of sale is encrypted when it enters the Steak n Shake system, but the data only

resides in the system for a limited time. Steak n Shake transfers nightly data batches to its financial acquirer across a private network, at which time the credit-card data is wiped from the Steak n Shake system.

"Another part of our overall strategy is to roll out an awareness program to bring employees up to speed on policies and procedures," stated Smith. "Employees need to understand what credit-card data is, that the privacy and security of this data is critical, and what they are and are not allowed to do with it."

Although the past year has been a whirlwind of new process and system implementations to meet PCI compliance, Smith said the timing was advantageous in at least one respect. "We were fortunate that the notification came in August before we had completed the budget process for this fiscal year. Our fiscal year begins Oct. 1, so we were able to plan for the necessary investments."

Initially, Steak n Shake proposed a two-year remediation plan. However, when Visa announced that its merchants had to achieve compliance by this month (September 2007), it forced Steak n Shake to escalate the plan.

"We expect to complete the testing and rollout by the end of August and submit our report in time to meet the September deadline," Smith told *Chain Store Age* in a July interview.

In light of the risks associated with failing to meet PCI compliance, there was a brief moment when they questioned if the restaurants should continue to accept credit cards. But it was only a moment, as Smith declared, "It would probably put us out of business if we did not accept credit cards."

Currently, the chain only accepts credit-card transactions and does not accept debit cards. However, debit cards will likely be added in the future. Additionally, Smith said the company has looked at technologies that allow contactless payments through RFID-enabled cards or mobile handheld units that enable customers to retain possession of their cards during the swipe. ■

—cgentry@chainstoreage.com