



In December 2010, **Merchant Link** announced the launch of its next-generation Merchant Link Payment Gateway, offering merchants more flexibility in processing and managing electronic transactions. An ideal solution for the restaurant sector, the gateway now offers anywhere, anytime cloud-based batch management and advanced tokenization and point-to-point encryption, and is easier for merchants and software providers to implement. It is a secure, high-speed payment network that connects a merchant's POS terminal and payment processors.

With cloud-based batch management, Merchant Link customers can control the batch management process centrally and from any location with a secure Internet connection. The solution includes TransactionVault, Merchant Link's tokenization technology that replaces each card number with a token, and TransactionShield, a point-to-point encryption product.

According to Tim Kinsella, executive vice president of sales and marketing at Merchant Link, there are two points at which data can be especially vulnerable. Data in-flight through corporate infrastructure, or transferring from the merchant to the processor and to the payer, is best protected by Merchant Link's TransactionShield. Data at rest, or stored data, is best protected by Merchant Link's TransactionVault.

"These two solutions used in tandem offer a layered approach," Kinsella says. "There is a need to protect cardholder data throughout the entire transaction life cycle. The only safe place for data is where the bad guys aren't looking for it."

The updated gateway now uses card-based tokens that extend beyond traditional transaction-based tokens and protects cardholder data. This allows merchants to track participation in loyalty programs and other marketing analytics. All cardholder data is still removed from the merchant's IT environment—dramatically reducing the risk of a data breach.

Kinsella says that, for safety reasons, data shouldn't be decrypted in-house. Merchant Link decrypts the data in the

cloud, then sends it back as a token. The best scenario is one in which the merchant has no access to plaintext cardholder data or to the cryptographic keys (in other words, no ability to decrypt the encrypted data). This frees the retailer of the risks of keeping data secure while removing portions of the merchant environment that require PCI validation.

"We host the information and are in the center of the transaction flow," Kinsella says.

Fifth Third Processing Solutions took an innovative approach to addressing the unique needs of their customers with an enhanced Host Data Capture (HDC) solution. As one of the industry's top processors, it handles millions of transactions a year.

Fifth Third developed the HDC solution to improve transaction processing for tip adjustments and help prevent batch upload failures and lost batches that continually cause issues for restaurants. Taking the HDC development further, Fifth Third realized it could help these merchants eliminate the need to store card data on their system, a major bonus from the PCI Compliance and data security perspective. With transaction data captured and stored on the Fifth Third Processing Solutions' host, merchants are able to use other system-generated transaction information to not only adjust transactions for tip, but to also initiate reversals and void transactions. Taking card data storage out of their system and still having the ability to easily perform key POS transaction functions for credit, debit, EBT, and gift cards helps improve the restaurant's oper-

ating efficiencies and bottom line and helps reduce the risk that card data can be compromised in the merchant's system.

WiFi or not, for merchants it certainly makes a lot of sense to rely on a company that specializes in security to handle PCI compliance and all it entails. It is far too complex for the typical operator, whose expertise lies in running a restaurant. However, it behooves merchants to take the time to educate themselves in at least the basic of compliance, says Brad Cyprus, senior security architect at **Vendor Safe Technologies**, a Houston-based provider of secure networks.

"Nobody can make someone else compliant," Cyprus says. "Everyone should have some knowledge and education about PCI and how it works."

Cyprus says online educational courses for general PCI knowledge for both operators and their employees is time well spent. "Understanding the requirements expected of the operator is a good step forward," he says.

Vendor Safe Technologies specializes in providing merchants with everything they need to complete their PCI compliance efforts. This includes managed firewall services, monitoring, policy and procedures, secure remote access options, and more. Vendor Safe differentiates its services by also offering the technologies merchants struggle with most often. Cyprus says an example of Vendor Safe going beyond other solutions is its Rogue Wireless Access Point Detection, which includes the wireless scan and report merchants need quarterly to determine if their environment has been compromised by an unauthorized access point. Vendor Safe also has developed its own software known as LanScribe that is specifically designed to help merchants comply with the local logging and file integrity monitoring services as stated in the PCI standard, without requiring customers to be computer experts. Lastly, Vendor Safe completes the PCI picture with the VST Internal Vulnerability Scan, a proprietary scanning engine that checks a merchant's susceptibility to intrusion without installing any new software or hardware at a customer's location. Vendor Safe is a security vendor with so much confidence in its solutions that it backs them up with a \$100,000 breach prevention guarantee, called the TrustVault Certificate, in writing.