

Protecting Diners and Restaurant Operations

What's On the Menu? PCI

Restaurants large and small are equally bound to comply with PCI payment security mandates.

Achieving PCI compliance and preventing card skimming may be easier than you know.

Content

Introduction	Page 3
Table Stakes are High	Page 3
What it Means to be PCI Compliant	Page 4
Compliance Required at All Levels	Page 6
Achieving PCI Compliance	Page 6
Implementing PCI Compliance Standards	Page 7
Preventing Skimming	Page 7
Bringing Payment to the Point of Service	Page 8
ON THE SPOT Solutions: TablePAY and CarsidePAY	Page 8

Introduction

Restaurants are a prime hunting ground for criminals intent on stealing credit card numbers and personal identities. High volumes, complexity of operations, and the large number of individuals involved in typical transactions present multiple opportunities for compromise of cardholder data.

Dining establishments are one of the few remaining environments where transactions occur out of sight of the card holder, creating the potential for a practice known as card skimming. Many establishments may also be using older point-of-sale systems that stores cardholder data in violation of the rules established by credit card brands. And others are using outdated card acceptance terminals that are prone to tampering.

This white paper examines the potential for fraud in restaurants and provides an overview of industry mandates that govern how merchants are supposed to ensure security for credit and debit cards.

Table Stakes are High

As electronic payment by credit and debit card has increased in transaction volume and dollar value over the past two decades, it has become the target of rising fraudulent activity by individuals and sophisticated gangs who would like to take advantage of any gaps in security. Criminal elements are constantly probing for the weakest link in the payment chain in order to extract the greatest gain for the smallest expenditure of effort.

While card data breaches at major retailers such as TJ Maxx (TJX) and DSW Shoes have generated the lion's share of headlines, incidents of card theft at restaurants large and small have been disturbingly frequent.

Restaurants in major cities from Los Angeles to New York, and smaller venues from Springfield, IL, to Hanover, N.H., have felt the ire of patrons who have found the card accounts purloined by criminals. In 2007, law enforcement nabbed a gang that reportedly skimmed cards at more than 40 establishments, including in Manhattan's Chinatown and other parts of the New York metropolitan area, as well eateries in Florida, New Hampshire, New Jersey and Connecticut.

According to industry estimates more than 40 percent of all card fraud originates in restaurants. Trustwave, a leading provider of on-demand data security and payment card industry compliance management solutions, reported

that of the 350 incidents it investigated, more than 54 percent involved restaurants.

Card skimming is one of the most common types of fraud impacting restaurants. Skimming involves making a copy of a card's magnetic stripe data, then using that "skimmed" data to create a bogus card and charge hundreds or thousands of dollars to that cardholder's account, before he or she receives the next statement. A dishonest server could use a small, easily concealable device to read and capture the card data while out of sight of the cardholder.

Another form of fraud is a result of hackers gaining access to older restaurant management point of sale systems that do not comply with requirements safeguarding cardholder account information.

The major card brands have established penalties to ensure compliance with industry security mandates. Failure to comply can result in penalties, including fines and other sanctions regarding the ability to accept card payments. For example, Visa levied \$880,000 in penalties against the bank that processed transactions for TJX, reasoning that the bank was complicit in allowing non-secure practices.

While Visa does not have the jurisdiction to fine merchants, it can fine processors and acquirers who in turn may levy contractual penalties on their customers. In addition, as was the case with TJX, banks can sue merchants to recover the costs of issuing replacement cards.

In addition to the penalties, there is also the potential damage to the relationship between an establishment and its customers. According to a new study by Javelin Strategy & Research of security breach victims, 55 percent expressed reduced trust in the breached organization's ability to protect and manage their account information, and 30 percent said they would never again purchase goods or services from the affected organization. Industry experts say it may take years to regain customer loyalty once it has been lost, if it can be regained at all. Maintaining security standards is extremely important today and is particularly relevant in the restaurant environment where most establishments haven't yet made the switch to pay-at-the-table or carside payment solutions.

What it Means to be PCI Compliant

There are some simple steps operators can take to protect their customers, their sales and their good brand name in a very competitive environment.

The most practical – and often most misunderstood – step is to become PCI compliant, a term most restaurant owners have heard or read about by now that stands for Payment Card Industry security standards. The PCI standards apply to

every organization that processes credit or debit card information, including merchants and third-party service providers that store, process or transmit credit card/debit card data.

Initially forged by the major card brands, including Visa and MasterCard, the PCI standards are now governed by an industry association called the PCI Security Standards Council. VeriFone is proud to be the only payment technology vendor that sits on this council.

The council maintains three key standards that mandate the use of credit and debit card account data:

- PCI PED (PIN Entry Device) governs any payment terminal or device that includes a PIN entry device by which a consumer can key in his or her PIN, or personal identification number, that verifies to the electronic payment network that he or she is authorizing a transaction against their checking account. Payment terminal suppliers such as VeriFone may no longer sell devices for PIN usage that are not PCI PED approved. Merchants can continue to use older systems that comply with an earlier Visa PED standard, but are urged to upgrade to PCI PED approved systems as soon as possible. Pre-Visa PED systems will have to be removed from service in 2010.
- PCI DSS (Data Security Standard) is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. It mandates such things as use of firewalls and antivirus software, the encryption of card data over public networks, protecting stored card account information, restricting physical access to card data and monitoring access to card data, as well as other requirements.
- PA-DSS (Payment Application Data Security Standard) is the newest standard from the council and is based on Visa's earlier Payment Application Best Practices. PA-DSS provides guidelines to software vendors and others on developing secure payment applications that do not store prohibited data, such as full magnetic stripe, other sensitive authentication data or PIN data, and support compliance with the PCI DSS.

Compliance Required at All Levels

Until recently, most attention was focused on larger merchants classified as Level 1 and Level 2 by Visa. Those categories were based on the number of card transactions, with Level 1 merchants handling more than 6 million annually and Level 2 handling from 1 million to 6 million annually. Visa required acquirer organizations to validate annually that those merchants were in compliance with its Cardholder Information Security Program (CISP).

As those larger organizations have increasingly come into compliance with the various requirements for handling card account data, attention has turned to ensuring compliance among smaller organizations. Level 3 merchants—those handling 20,000 to 1 million transactions—and Level 4 merchants who deal with less than 20,000 transactions annually, are moving into the spotlight. Visa says that Level 4 merchants are cumulatively responsible for less than one third of all Visa transactions, “but account for more than 99 percent of the merchants that accept Visa.”

Therefore, says Visa, “cardholder data compromises affect Level 4 merchants with greater frequency than Level 1, 2 and 3 merchants combined.” In fact, 80% of identified compromises since Jan. 1, 2005, have occurred at Level 4 merchants. Visa now requires acquirers to develop risk assessment programs to identify and manage risk among their merchant populations. Under this program, acquirers may require even the smallest merchants to undergo a quarterly network scan to identify security problems.

Achieving PCI Compliance

Today, savvy restaurant operators of all sizes realize that the stakes are high and without PCI compliance, business risks can be great. Merchants can be fined and held responsible for charges associated with card replacement costs and providing consumers with ID theft protection for those who were compromised. Not to mention loss of reputation costs once the security breach information reaches the headlines.

Meeting PCI requirements can be hard for restaurants struggling to keep up with security requirements, which are sometimes difficult to implement, maintain and monitor. However, the payment industry has developed a wide array of new PCI compliant products that both help restaurant operators to

ensure secure card practices and make it easier to validate that they are in compliance.

Additionally, there are many service professionals available who can help with PCI certification and provide guidance as to how to maintain maximum security so that merchants remain compliant at all times.

Implementing PCI Compliance Standards

There are numerous technical and administrative tasks associated with implementing PCI compliance standards. Below are some tips to make the process easier:

- Set clear business policies for your employees regarding the processing of credit/debit and payroll card data. Many security breaches actually happen within an organization, so it is critical that policies are clear to employees.
- Update your employees regularly with new or different measures being used to ensure PCI compliance. Make sure that you keep your employees up-to-date on any changes made that affect the security of the data you store or transmit.
- Keep records of how your business is complying and validating the PCI standards. Remember that you will be audited. Keeping good records will assure your company will remain in good standing with the credit card companies.
- Be involved in all IT decisions regarding how your business will comply with the regulations.

Preventing Skimming

As discussed earlier, a common form of card fraud in restaurants is the practice of skimming. Fraudsters run a card through a very small, concealable magnetic stripe reader that captures the cardholder data, which can then be cloned and/or sold over the Internet for the purpose of unauthorized purchases. These devices are readily obtained and are so easy to use and conceal that a server could readily capture the card data while walking from the table to the cash register.

Restaurants and other hospitality businesses were among the earliest adopters of standard forms of electronic card payment. Yet despite advances in card acceptance in other industries—such as quick serve restaurants, groceries

and even convenience stores—today’s hospitality business typically utilizes a cash register or standalone POS terminal that sits in a fixed location. Every credit and debit card transaction requires multiple steps to complete, with customers first waiting to receive their check, handing over a card, waiting for it to be taken to a counter or backroom, and finally being handed a receipt to sign.

As consumers grow increasingly weary about card security—and desire to use PIN debit cards—more and more merchants are looking to accept payment at the point of service. Portable payment solutions virtually eliminate the possibility of card skimming while increasing speed of payment and improving customer service.

Bringing Payment to the Point of Service

High-speed, wireless and IP-enabled solutions at the point of service allow consumers to keep their credit or debit card in hand while restaurants and hospitality businesses take full advantage of the lowest cost processing options. The solutions improve the efficiency of servers and counter clerks, freeing up their time to focus on serving the guest instead of processing payments.

Recognizing the challenges facing restaurant operations, VeriFone developed its ON THE SPOT payment solutions to bring secure, efficient payment solutions right to the point of the transaction. VeriFone developed a range of solutions to fit restaurant’s needs, from the table to the counter, the car, or the front door.

ON THE SPOT Solutions: TablePAY and CarsidePAY

VeriFone developed ON THE SPOT solutions to address payment issues in the restaurant environment. A key requirement was delivery of PCI PED approved security in a customer-facing portable payment solution that was “purpose built” to meet the needs of servers at the table, as well as for takeout service at the curb. The result was the VeriFone V^x 670, a TablePAY and CarsidePAY portable payment solution that is highly suited for any environment, with a rugged case that is impact-resistant and spill-resistant to endure the most demanding conditions.

The V^x 670 is a wireless system that is available in cellular CDMA and GPRS versions as well as WiFi to meet the particular needs of any restaurant operation. Security was a paramount design parameter for the V^x 670, which meets all current requirements for PCI PED devices. CDMA and GPRS have proven to be highly secure communications technologies and the V^x 670 WiFi version utilizes WPA-PSK (pre-shared keys) to protect WiFi transactions.

No transaction data is stored in the V^x 670 and customer PINs are never transmitted without additional encryption. In addition, VeriFone's VeriShield architecture prohibits rogue applications from being loaded onto the V^x 670.

Restaurants use one of several methods to submit card transactions. Some utilize restaurant management systems; others a standalone dial up service. VeriFone makes it possible to utilize the V^x 670 in a number of ways:

- Integrated with leading RMS, including MICROS, Aloha/Radiant and POSitouch.
- Utilizing a managed service that allows restaurants without an RMS to simultaneously use multiple devices and enjoy some RMS-like features, including transaction consolidation, terminal and transaction management, reporting, and automated settlement service. VeriFone's ON THE SPOT Managed Services Portal offers web-based, real-time and historical reporting from any PC with Internet access.
- Standalone use, utilizing cellular GPRS, CDMA or WiFi to communicate on a device-by-device basis to a payment processor.

The VeriFone Difference

Under the PCI mandates, merchants are responsible for the physical security of their payment devices and the actions taken by their employees. VeriFone's revolutionary ON THE SPOT payment solutions protect restaurants and customers by enabling secure payment at the point of service, harnessing the power and flexibility of secure wireless technologies. From the table to the counter to the car to wherever your patron is, VeriFone has an ON THE SPOT solution to fit your specific business needs for safe and secure card payment.