

Payment Card Data Security for the Restaurant Industry

"Be careful with your personal information. Be careful who you give your credit card to. It's just as vulnerable in a restaurant as it is on the Internet."

— Howard Beales, director of the Bureau of Consumer Protection from 2001-2004

Beales sounded this warning in 2003 during an interview discussing the Federal Trade Commission's (FTC) efforts to prevent identity theft. At the time, it's likely Beales was referring to small-time "skimming" (e.g. a waiter stealing a small number of credit card numbers by keeping a copy of a receipt with the full card number and expiration date printed on it, or simply writing it down). Little did he know that in 2006 this comment could be labeled as nearly prophetic—albeit with one variation:

Looking over a large number of security breaches at restaurants in 2005, we've found that payment card information is probably *more* vulnerable at a restaurant and other brick and mortar merchants than on the Internet. And just as a restaurant is *more* vulnerable, today's thieves steal *more* payment card information through even smaller, and seemingly insignificant, holes.

In a typical security breach at a restaurant, an attacker will steal cardholder information for approximately 40,000 cards—a far greater number than in a typical skimming incident. And the individuals involved in these types of thefts are more than just rogue waiters. In many instances, these attackers work for a larger international organization that uses the stolen card information to create counterfeit credit cards. These copied cards use the account information encoded on the original card's magnetic stripe and are then sold on the black market or online. An individual case of credit card fraud devastates its victim, but theft on the scale mentioned above devastates not only the cardholders, but also the business to which a compromise is traced.

Over the past year, security breaches have been regular front page news. If a company or restaurant is included in one of these stories, consumers get the impression that the company does not handle personal information in a secure or protected manner, and they will think twice before patronizing that restaurant. And as any restaurant manager or small business owner that regularly examines the daily numbers knows, the percentage of consumers that prefer to pay by card continues to increase. While a number of fine-dining restaurants have always accepted cards, now even quick service restaurants accept credit cards, *and* PIN-secured debit payments. With the proliferation of payment card acceptance across all dining categories, acceptance is hardly optional for any restaurant trying to compete in the market. Consumers *want* to pay by card, and if their card information is stolen at a particular restaurant, it's not likely they'll be back. It is likely, however, that they'll tell their story to others. Plus, with consumer notification laws, such as California's SB 1386, in many cases a business *must* notify consumers if their information has been exposed in a breach. Soon enough, a security breach has emptied a restaurant's tables and tills as quickly as a case of food poisoning. A security breach at a restaurant is an expensive proposition.

Just one breach, no matter its severity, at one franchise location can damage the reputation of an entire brand. Consumers are not likely to differentiate one chain location from another—if one location is breached, in the consumer's eye the entire corporate brand is tainted.

Loss of business is not the only consequence of a security breach. The theft of cardholder information can seriously undermine the brand of a credit card association. Before 2004, to assure consumers of their brands' reputations as trustworthy payment options, each of the major card associations (Visa, MasterCard, American Express and Discover) drew up individual data security programs that they required merchants follow in order to accept their card brand. As one might imagine, the process of ensuring that merchants complied with four different, yet equally complex, security policies proved impossible for many merchants. To alleviate this issue, in December 2004

Visa and MasterCard announced the creation of the Payment Card Industry Data Security Standard (PCI DSS)—both American Express and Discover are in the process of endorsing the standard. Though specific requirements will be discussed in detail later on in this paper, in brief the PCI DSS requires that merchants build and maintain a secure network, protect cardholder data, maintain a vulnerability management program, implement strong access control measures, regularly monitor and test networks, and maintain an information security policy.

All card associations require that any member, merchant or service provider that stores, processes or transmits cardholder data must comply with the PCI DSS. This includes any restaurant that accepts payment cards, no matter how small the transaction volume. While the previous statement may seem obvious, we've found that many restaurant owners and managers simply never realized this fact until it was too late. Not complying with even just one requirement could, in the event of a breach, lead to fines and expulsion from the Visa, MasterCard, American Express or Discover networks.

In our work we've found that many restaurants are unaware of data security-related issues and as a result, put PCI compliance near the bottom of their priority list. Often a restaurateur receives a letter from their acquirer that uses words like "encryption" and "firewalls," and suggests they take a look at Visa's Web site for more information about PCI compliance. But that restaurateur may dismiss the information as just so much techno-babble. They may pay little or no attention to the information, figuring it has little or nothing to do with running a kitchen or dining room. In some ways they're right. There's no need to encrypt a cut of meat or set up a firewall to preserve the integrity of data stored on the salad line. Nor is it necessary to ensure a table setting is compliant with anything but eating comfortably. However, if a restaurateur wants to keep meat in the cooler and greens on that salad line, it's imperative they take PCI compliance seriously.

Typically, indications of a possible breach do not originate at the business site—they start with the cardholder;

1. Cardholders will inform their card issuers of possible fraud on their accounts.
2. The card issuers relay this information to the card associations to determine a common point of purchase (for instance a quick service restaurant where all of the compromised accounts made purchases during a particular period of time).
3. Once this point is determined, the card associations contact the merchant's acquiring bank (who handles the merchant's card payments) to inform them of the possible breach. The merchant may then have to submit to a forensic investigation performed by a qualified assessor. A forensic investigation alone can cost \$7,000 to \$12,000 or more.
4. The assessor submits a report detailing whether or not there is evidence of breach of the merchant's systems, possible causes of the breach, and whether the merchant was PCI compliant when it occurred. Non-compliance is a major factor in determining whether or not the card associations will impose a fine and the amount of the fine levied. Fines for non-compliance can be as high as \$500,000, and the card associations can also require the liable party to pay for re-issuing compromised cards (running anywhere from \$25 to \$50 per card).
5. If the assessment confirms a security breach, the card association will fine the compromised merchant's acquirer since it is their responsibility to ensure their merchants are compliant with the PCI DSS. Typically, an acquirer's contract with a merchant will spell out in no uncertain terms that the merchant is liable should a data security breach occur at their place of business. This means the costs of the investigation, re-issuance, and fines all fall to the bottom of the payment chain – in this case, the restaurant.

Many times, restaurateurs assume responsibility for PCI compliance lies elsewhere in the payment card chain. A number of entities contribute to a restaurant's ability to accept payment cards—the developer of the software used for their POS system and restaurant management, the POS terminal manufacturer, the merchant's acquiring bank, the merchant processing company (hired by the acquirer to process card payments) and the integrator that installed the entire system on site, not to mention any additional third parties hired by any company along the way. It would disturb many consumers to learn that we find many restaurants avoiding data security issues altogether by relying on third parties and hosting providers to handle the technical aspects of their business. It's possible these third parties themselves are not even aware of PCI, let alone qualified to explain, interpret or validate compliance. Even worse, a transaction processor, POS vendor or hosting provider may misrepresent their systems or services claiming they are PCI compliant. Since there

are thousands of processors and POS applications, when shopping for a system that allows them to accept payment cards, a restaurateur can always find a vendor that claims they are less expensive. Any company in the payment card industry wants to maximize even the smallest of profit margins, many times forgoing the up-front costs to ensure compliance. This can prove disastrous because while at first glance these POS terminals are indeed less expensive, if the POS system purchased by a restaurateur isn't on Visa's list of validated payment applications, that restaurateur can't be sure that their environment is PCI compliant.

In many of our investigations, we find that when a POS system is to blame for a security breach, it's because the system did not operate in accordance with the Payment Application Best Practices (PABP) guidelines (Visa's set of standards for payment application data security). For instance, the system may have stored full track data (the information encoded on a payment card's magnetic strip) in log files or databases. This information is a wellspring for hackers who know that more often than not, they'll find these sorts of mistakes at smaller merchants.

Thus far, the card associations have concentrated their efforts on larger entities and their compliance with PCI standards, leaving restaurants in the level four category to fend for themselves. This is illustrated by the different validation requirements for level one, two and three merchants compared to level four merchants. While the card associations emphasize that PCI compliance is absolutely mandatory for all organizations that process, store or transmit credit information, thus far they haven't required level four merchants to **validate** their compliance except in special cases such as after a compromise. Hackers know this and target smaller merchants (especially restaurants, as they're likely to accept payment cards and use wireless technology) knowing they may not even be aware of vulnerabilities in their systems. In our experience, a restaurateur isn't aware they've been compromised until weeks after the breach.

The card associations have started to realize that level four merchants are as much, if not more, at risk as level one merchants, and our work in 2005 attests to this fact—the majority of our card compromise investigations were at retail and restaurant locations. Given the number of level four merchant breaches and the number of cards at risk, it's probable that the card associations will increase their vigilance over level four merchants and begin requiring validation of PCI compliance. To plan for this probable change, restaurants need to understand what PCI compliance requires, determine whether their payment environment meets those requirements and, finally, implement any necessary remediation. This is important not only to preempt the possibility of mandatory validation, but also to ensure that a restaurant protects its most valuable asset—its relationship with its customers.

In our investigations of data compromise involving restaurants, we find that more often than not three major issues led to the compromise:

1. Cardholder data is stored on an Internet-connected server;
2. Vendor-supplied defaults are used for system passwords; and
3. POS systems and terminals do not follow Payment Application Best Practices guidelines

In most cases, not only is a restaurateur unaware of the risks, but neither are the third parties that develop, install and maintain their systems. All three of these issues could have been prevented had the restaurant been PCI compliant; saving them time, money, and customers.

Suggested Best Practices for the Restaurant Industry

While all merchants must adhere to the entirety of the PCI Data Security Standard, we've found that the majority of restaurants fail in several key areas:

- **Protecting cardholder data**, by not ensuring the security of stored data and encrypting the transmission of that data across public networks
- **Maintaining a vulnerability management program**, by not developing and maintaining secure systems and applications
- **Implementing strong access control measures**, by not assigning unique IDs to all employees with computer access
- **Regularly monitoring and testing networks**, by not tracking access to network resources and cardholder data and failing to test security systems and processes
- **Maintaining an information security policy**

Examining a small sample of recent forensic investigations, we've found that restaurants' most common violation of the PCI DSS is the storage of unencrypted track data by their POS system. Track data is the information encoded on a payment card's magnetic stripe and is exactly the sort of information a hacker is after. There are a number of tactics restaurateurs can implement to ensure they and their customers are protected from hackers:

- **Obtain a PCI-compliant version of software for POS system** - Confirm that your POS system is indeed PCI-compliant and that you've installed the latest software updates. If a vendor cannot verify that their payment application is PCI-compliant or does not appear on Visa's list of validated payment applications, switch vendors. Ensure that the contract with a new vendor requires their system follows the PABP guidelines and is PCI compliant.
- **Encrypt cardholder information** - Be sure your system can encrypt both stored data and data sent over public networks. PABP-compliant systems already do this. As previously stated, many vendors misinterpret the PABP as well as the PCI, so a restaurateur must confirm this with their vendor.
- **If switching to a new software version, or POS system altogether, be sure to remove any backup data directories created by non-compliant systems** - When a restaurant implements a new update or patch for their POS system, or an entirely new system, sometimes the uninstall process is left incomplete. The very reason the new system is implemented, because a previous system stored unencrypted track data, is not actually addressed because the previous system's storage directory is not removed.

Yet another area of PCI compliance many of our restaurant clients have struggled with is developing and maintaining secure systems and applications. This can be as simple as installing the latest service pack from the Microsoft Web site or as complicated as upgrading your entire operating system (one of our clients had been using Windows 98 even though it was no longer supported with security patches by Microsoft). Even the smallest vulnerability in your system can give hacker's access to cardholder data. The following are suggestions to help you protect your systems:

- **Monitor vendors' Web sites for news of security patches for their applications** - This includes the Microsoft update Web site and the vendor Web sites for all applications used in a restaurant's environment. The PCI DSS requires that all relevant security patches are installed within one month of release. Many vendors provide both desktop and e-mail alerts for security patches and updates.
- **Use an anti-virus tool on all computers and servers** - Ensure that these devices are running, updated regularly and record audits. Many anti-virus vendors offer automatic updates of their applications or e-mail alerts. Viruses and malicious programs change everyday and your anti-virus program must be up-to-date as well to defend against them.
- **Stay apprised of the latest in data security vulnerabilities and ensure the security measures in your environment address them** - Many anti-virus vendors, and even the U.S. government, provide free weekly e-mail alerts and newsletters discussing the latest in security issues and vulnerabilities

We've also found that many restaurant environments do not limit or log the access of its many users. Because of this, a restaurateur may be granting an employee access to areas of the network that contain cardholder data—access they don't need to perform their daily duties. This explicitly violates the PCI DSS. Additionally, if an internal breach were to occur, without a log of each user's access to relevant systems, it makes it very difficult if not impossible to determine how cardholder data was compromised. Fortunately dealing with this situation is relatively simple.

- **Assign a unique ID and password to each person with computer access** -This covers two PCI requirements with one implementation; system administrators can restrict access to card data on a need-to-know basis, and identify which employees have access to credit card information. This is the first step toward the recommendation below.
- **Maintain user privileges and settings** - Regularly eliminate inactive accounts and those of terminated employees. Lock out a user ID after repeated log-in failures until an administrator re-enables it. These measures will ensure that only authorized users are accessing your network
- **Log any and all access, including that of users with administrative and root privileges** - A log will allow a system administrator to quickly recognize any irregularities

in network access and also save time and money when determining the cause of a compromise.

- **Monitor the logs and investigate any irregularities** - Catching an unauthorized user attempting to access your system can identify vulnerabilities that need to be secured in an environment before the attacker is able to exploit them.

Hackers pay close attention to the latest in technology developments. Whether it's hardware or software, a hacker sees a new technology as a test of their skills; and barring discovery or prosecution, they don't give up until they've passed that test. We have seen a number of restaurants employing new remote access software for inventory and other tasks; however, they fail to install the program securely and test its security controls. In one incident, a hacker remotely accessed a restaurant's network with a wireless-capable PDA device, possibly from the parking lot. If the administrator had tested the remote access software settings, they likely would have noticed the settings violated even the most basic security policy.

- **Regularly test all controls, connections, hardware, and software in your environment** - Ensure that your system is able to adequately identify and stop unauthorized access attempts. If wireless devices are used, periodically identify all wireless devices.
- **Perform internal and external vulnerability scans at least quarterly** - In addition to vulnerability scans, penetration testing should occur at least once a year. The scans and penetration testing should also be performed after all significant changes in your environment since the addition or removal of software or hardware can open access points in your system.
- **At least daily, monitor your environment to compare critical files and alert personnel if any unauthorized modification occurs** - A critical file is not necessarily one that contains cardholder data, but one that does not regularly change. Inconsistencies in compared files can indicate that a breach has occurred.

This final suggestion is possibly the most obvious and easiest to implement; however, we've found that the majority of restaurants haven't yet accepted its importance. Every restaurant should develop and implement a restaurant-wide security policy that covers all of the PCI standards. Any security effort must truly involve the entire organization so that all employees understand the importance of protecting cardholder data and what they can do to ensure its security.

- **Write, publish, maintain and disseminate a security policy addressing all of PCI** - This will inform employees of the security stance at your restaurant and also provide a plan of action and a standard by which to measure your progress. The entirety of the PCI may seem intimidating, or at least abstract, but once a concrete security policy is in place, it's that much easier to maintain and enforce.
- **Include user policies for the technologies employees will be using** - Require that employees receive explicit approval from management to use these technologies and create a list of all devices and which employees have access. Be sure to outline the appropriate uses for these technologies.
- **Review security policy annually and make changes when necessary** - A yearly review will provide the self-assessment necessary to assure that your compliance with the PCI DSS is not just a one-time event, but a continuing effort to protect yourself and your customers. While you should perform this review at least every year, also review your security policy when adding software or hardware to your environment (including internal and external scans and penetration testing).
- **Implement a security awareness alert system that informs employees of changes to the security policy and other data security issues** - These alerts should also include reminders of specifics within the security policy and how employees can contribute to the overall security of your environment's cardholder data.

Conclusion

The suggestions above are general recommendations based on the PCI Data Security Standard and our experiences in the field. This should not be considered a comprehensive list. In the end, working with a data security company that specializes in compliance with the PCI DSS, such as

AmbironTrustWave, is invaluable. Working with *qualified* and *certified* data security experts will instill confidence in your customers that they can trust you to protect their card information while allowing you to concentrate on producing culinary delights rather than PCI compliance and reduction sauce rather than encryption and firewalls.

This paper opened with a quote that confirmed trends we noticed in 2005—that restaurants and retailers are a popular target for data compromise. Because of misinterpretation or lack of knowledge regarding data security issues, reliance on third parties inexperienced with PCI compliance, or insecure POS systems, restaurants are especially at risk. Consumers will spend their money only where they trust their personal information will be secure. Ensuring your restaurant's compliance with the PCI standards can earn or maintain that trust and protect you and your customers. AmbironTrustWave is available to assist you and your restaurant in these efforts to reduce your exposure to security incidents and loss of sensitive information, enhance your organization's security posture, manage your institution's complex credit card processing environment, improve merchant network security, and demonstrate compliance against industry and regulatory standards.

About AmbironTrustWave

AmbironTrustWave is a leading provider of information security and compliance management solutions to businesses in the Fortune 2000 and the public sector. The company's flagship products, TrustKeeper® and TrustMinder™, serve more than 25,000 businesses throughout the world to validate compliance with a variety of industry standards and regulations. For the payment card industry, AmbironTrustWave helps banks, merchants, service providers and software developers mitigate their risk by validating compliance with industry best practices for safeguarding information endorsed by American Express, Discover, MasterCard, Visa Canada and Visa USA. AmbironTrustWave clients include financial organizations, global electronic exchanges, educational institutions and business services firms. The Company also provides services to several government agencies. AmbironTrustWave is headquartered in Chicago with offices throughout the United States.