



Fighting fraud is an ongoing battle. Are you at Risk?

Did you know that you are liable for data you have? Are you aware that hackers are testing your security every day? The sophistication of fraudsters and the methods they employ increase all the time. The threat is becoming increasingly organized, international and professional. As awareness of protecting financial information grows, all stakeholders in the payment system are concerned about preventing identity theft, database hacks, card skimming, phishing and other fraud schemes that surface.

Payment Card Industry (PCI) Data Security requirements marks a watershed moment in the payment services industry. With the common goal to protect the cardholders, PCI standards apply to all members, merchants and service providers that store, process or transmit cardholder data. Based on well-known security practices and common sense, compliance with the PCI Data Security Standard will help preserve the integrity of the payments system and maintain consumer confidence.

You only have to read the newspaper headlines to understand the negative consequences of data compromise.

- Adverse media publicity
- Loss of consumer confidence & damaged reputation
- Increase cost with exposure to notification expenses and liability litigation

With consumers looking to place blame for compromised data, the public impact is an outcry for legislation. The federal government is looking at notification laws for security breach, with a greater interest in restaurants & retailers and what they are doing to protect data.

By truncating the card account number on receipt copies, restaurant operators have some experience with rules and regulations protecting cardholder data. Depending on the size of the restaurant, they may be required to conduct an annual onsite audit, quarterly network scan and/or an annual self-assessment questionnaire. Unless a restaurant is doing more than six million transactions a year, they are not required to validate their compliance against the PCI standards but they are still required to operate in a manner that is consistent with them. Non-compliance could result in fines and penalties if stored data is compromised.

The greatest risk to a restaurant merchant regarding account compromise is whether or not their Point of Sale application is storing mag-stripe data. If so, they are unnecessarily exposed to account data compromise. All discretionary card-read data, card verification data, PIN data, and address verification (AVS) data should not be saved. Failure to adhere to this standard can have significant consequences. Once an authorization is received there is no reason to store this data. Additionally, if they are storing data such as cardholder name, account number or expiration date they need to insure the data is securely protected. With the increase in using Internet protocol (IP)-based payment solutions to transmit transaction information, comes increased risk if your network is also connected to your database where you store cardholder and transaction information.

Vulnerabilities are simply a fact of life... The Top Five Causes of Data Compromise

#1 Ineffective Patch Management.

In most cases a simple download of a publicly available software patch can correct a vulnerability and deter a potential intruder.

#2 No security scanning.

Intruders use scanning tools to find the path of least resistance into a network. For security professionals, scanning is an effective and inexpensive way to monitor and repair vulnerabilities that may be exploited by hackers.

#3 Weak Network Level Security.

Too often companies lack proper network segmentation, allowing intruders to enter and roam throughout the entire corporate system.

#4 SQL Injection.

This technique is used to attack the database query by injecting characters into it causing a break down of its defenses.

#5 Lack of real time security monitoring.

Criminals function after hours and weekends and with no real-time monitoring during these times intruders can attack without concern of detection.

The 12 Requirements of PCI Data Security

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data with encryption and keep storage to a minimum.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update anti-virus software.
6. Develop and maintain secure systems and applications.
7. Restrict access to data and limit access on a need-to-know basis.
8. Assign a unique ID to each person with computer access.
9. Restrict physical access to cardholder data and destroy media containing transaction information when it is no longer needed.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain an information security policy.

Ultimately, it is the merchant's responsibility to make sure their payment system is secure and that they are following the Data Security Standards laid out by the Payment Card Industry. Restaurants are required to make sure the Point of Sale (POS) application they are using does not store mag-stripe data. When shopping for a system or contemplating a system upgrade, this question should be asked. Vantage will help you research PCI compliance of your POS provider and application version. We can also recommend and refer you to security scan systems and consultants. Contact your personal point of contact or call us at 800-397-2380.