

## What Can I Do?

As a Level 4 merchant, you must be aware of data security issues in your business. Discuss the subject with your merchant card processor and the company that installed and/or maintains your POS systems and data networks in your stores. You can also follow these best practices:

- Ensure your POS software meets best security practices by one or more of the card networks and follows the network's "payment application best practices" and to be PCI compliant.
- Regularly update software and hardware with new versions and patches. If you use personal computers, install anti-virus tools on all systems and have a process to regularly install updates and be sure you are protected from unauthorized external access.
- Passwords for systems should be personalized and changed from the defaults to unique IDs and passwords for each user.
- Scan the network a minimum of once quarterly to identify problems. Certified approved scanning vendors perform the scans remotely to check whether your system can be breached. The PCI Data Security Standards Council lists certified vendors on its web site.
- Do not store unnecessary customer data. The PCI standards prohibit merchants from storing magnetic-stripe and PIN data, even in encrypted form.
- Conduct an annual self-assessment to determine your data security vulnerability.

If you are a Level Four Merchant (up to 1 million annual transactions) your best protections are to conduct an annual self-assessment, a quarterly network scan and ensure that you are not storing any unnecessary customer data.

## Who Can I Contact to Learn More?

PCI Compliance is a serious and complex issue, but there are many resources available. To learn more contact Tim Ehlert at the National Restaurant Association at (202) 331-5938 or [tehlert@restaurant.org](mailto:tehlert@restaurant.org).

A special thanks to Georgia Restaurant Association's General Counsel Charles Hoff for his guidance in the development of this information.

## Helpful Resources

### National Restaurant Association's Data Security Page:

<http://www.restaurant.org/business/datasecurity/index.cfm>

### PCI Standards:

<https://www.pcisecuritystandards.org/>

### PCI Approved Scanning Vendors:

[https://www.pcisecuritystandards.org/pdfs/pqi\\_qsa\\_list.pdf](https://www.pcisecuritystandards.org/pdfs/pqi_qsa_list.pdf)

### Visa USA:

<http://www.visa.com/cisp>

### MasterCard:

<http://www.mastercard.com/us/merchant/security%20/index.html>

### American Express:

<https://www.americanexpress.com>

Click on merchants.

### Discover:

[http://www.discovernetwork.com/resources/data/data\\_security.html](http://www.discovernetwork.com/resources/data/data_security.html)

Have You Budgeted  
**Six Figures**  
For a Potential  
Security Breach in  
Your Restaurant?



NATIONAL  
RESTAURANT  
ASSOCIATION®

## Are Your Financial Transactions Really Secure?

Restaurateurs can often times expect to pay in the range of six figures as a result of a data security breach—including credit card and card processing company fines and penalties, cost of forensic audit and expenses, credit card charge backs that can continue for 18 months after the initial breach, and the cost of reissuing customer credit cards. These charges are just the beginning and can pale in comparison to the prospect of lost sales or closing due to the erosion of confidence from customers.

PCI-DSS or “Payment Card Industry-Data Security Standard” refers to the data security requirements developed by the major credit card companies that all restaurants and merchants are contractually obligated to comply with in order to use VISA, MASTER CARD, AMEX and DISCOVER cards. The standards are designed to make it more difficult for external hackers to break into the restaurant’s systems and compromise their patron’s consumer credit and debit card information.

PCI-DSS has four merchant levels. Most restaurants are Level Four merchants, which means they process up to 1 million annual credit/debit card transactions. It is important for these businesses to understand their responsibilities and potential liabilities if their data security standards are not current and secure.

PCI compliance is no easy task. While there are only twelve fundamental components that make up the PCI standards, there are approximately 200 subcomponents and each of these standards evolve and are fluid in nature, so it is difficult to ever be confident of full compliance.

**4 out of every 10** cases of ID Theft occur from theft of sensitive credit card data information from restaurants with hackers specifically targeting restaurants due to their perceived vulnerabilities.

## What Happens in a Breach and What Will it Cost Me?

Restaurants rely on card processing companies and Point of Sale (POS) vendors to do their part in safeguarding data and prohibiting storage of magnetic stripe data from consumer credit card information.

The most common sources of problems for restaurants are with POS system software that is not updated to the latest compliant versions, or system networks which use “default” passwords that have not been changed. Or POS systems and networks use “default” passwords that have not been changed. Merchants commonly are found to have unsecured data networks exposed to the internet.

The highest risk restaurants are typically single location or part of a chain. They are predominantly card present, “retail” transactions. They use unsecured Internet-accessible store networks, like DSL, cable modem, or wireless technology. They also use non-compliant POS software that improperly stores card data elements.

Typically, when a breach is suspected, the restaurant owner/operator can expect the following:

- Receives a call from the Fraud Departments of the Credit Card companies to discuss incidences of irregular credit card usage within their restaurant that suggests the possibility of a security breach.
- The restaurant owner is compelled to promptly select from a short list of pre-approved forensic audit firms and be subjected to an intrusive internal security audit which can run from \$8,000 to \$15,000.
- With little or no notice, the restaurant’s card processing company is contractually permitted to begin withholding funds to pay for the projected fines, penalties and assessments.
- After completion of the forensic audit, a conference call is held with the owner, the card company fraud departments and the forensic auditor to discuss the findings and the restaurant’s remediation requirements (failure to follow the remediation steps will result in additional fines and possible prohibition of card usage).

- The restaurant is subject to fines, penalties and assessments ( credit card charge backs may continue for 18 months from the initial security breach. Fines could start as high as \$50,000 and merchants may incur monthly penalties beyond the initial findings until the matter is resolved.



Even if a forensic audit reveals that there have not been any PCI infractions, the finding of a single PCI violation such as an insufficient firewall or of easily detectable computer passwords could trigger fines and penalties.