

Restaurant PCI Basics

Restaurants are at high risk of credit card fraud. It's a risk that many restaurant operators underestimate – and many are too confused by the technical requirements to protect their businesses effectively.

Sound familiar?

In fact, while the risk is real, you can take action to protect your customers' cardholder data – and to safeguard your business from liability.



Learn the basics of PCI

The Payment Card Industry (PCI) standards have been established to help you safeguard customer information—and protect your business.

The basics of PCI are similar to the standard business practices you already use to safeguard your business: You lock your doors as a matter of course. To protect your customers' information, you also need the proper "locks" on your POS system and network.

Where to start? Read on to learn the key things you need to know about credit card security and PCI.

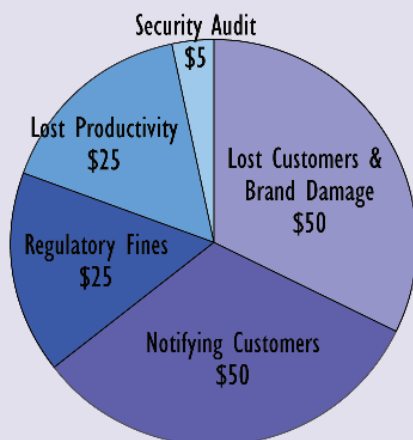


What is the cost of a credit card breach?

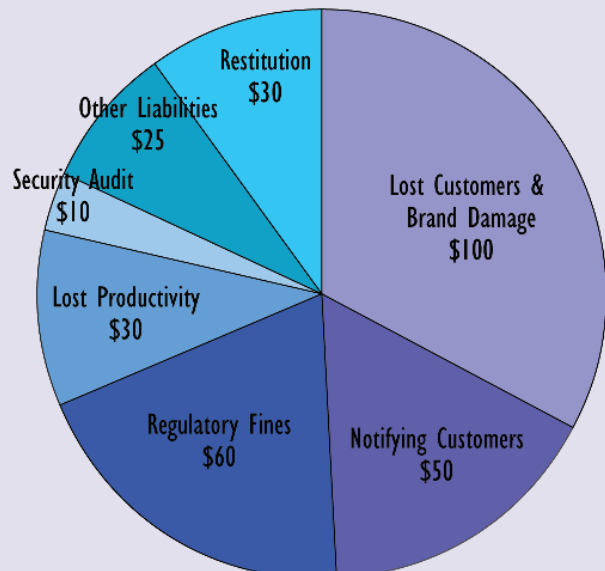
Estimating the cost of a data breach is not straightforward. In addition to the direct costs incurred in legal fees, security audits, fines, and penalties, there are also less tangible losses, such as brand damage, lost customers, and time spent dealing with the breach.

Forrester Research recently released survey data that estimated costs for low- and high-profile breaches. The graph below summarizes the firm's findings: In a regulated

industry such as food service, the cost can range from \$155 to \$305 for **each customer record stolen**. According to payment security consultant Trustwave, an average of 40,000 card numbers are compromised in a typical breach. But even in a breach involving less records, cost can escalate quickly and force a restaurant to close doors.



Low-Profile Breach
\$155 per customer record



High-Profile Breach
\$305 per customer record

Find out more

More on restaurants and credit card security: [Pasta, Meatballs and Credit Card Theft \(ABC News\)](#)

SecureWorks reports on [quantifying the cost of a breach](#)

How did you get to be liable?

When you signed a merchant agreement with Visa or MasterCard, **you agreed** to comply with payment card industry security standards. It's a single paragraph in the standard agreement that every merchant signs. But if a credit card breach is tracked to your restaurant, and you are unable to demonstrate compliance, that single paragraph could cost you more in fines and other penalties than your business can bear.

When you signed a merchant agreement with Visa or MasterCard, you agreed to comply with payment card industry security standards.



Restaurants Pay the Price

Who's more at risk of a cardholder data security breach? A large chain with a huge IT budget or an independent restaurant with little technical resources?

Global payment security consultant Trustwave reports that 9 of 10 cardholder data compromise incidents are aimed at small operators, such as restaurant and pub Spanky's Marshside, in Brunswick, Georgia.

In August 2006, hackers broke into Spanky's POS system. "Magnetic data was taken which I didn't even know we were storing in the hard drive, and new cards were made and sold over the Internet," said owner Carla Yarborough, in a video interview with the Retail Solutions Providers Association.

"I just felt I had been blindsided because I was not aware it could even happen," Carla said. She didn't learn of the breach until February of the following year. Hackers had the run

of her system for nearly seven months before suspicious transactions were tracked to her restaurant.

Like many operators, Carla didn't realize that her POS stored cardholder data, even though the information was no longer needed after the transaction has been authorized. "I didn't think I was at risk," Carla said. "I thought I had everything I needed because I had a brand new POS system and I thought that my software was compliant."

Trustwave reports that in 60% of the cases where data is compromised, merchants are relying on outdated software that improperly handles sensitive cardholder data.

Buying and maintaining compliant equipment is a crucial step toward protecting your customers from theft and your business from liability. "I think you don't have a choice," Carla said. "You can take the risk if you want to, but I'm sitting here as a witness that it can happen. The damages far outweigh the cost of upgrading your system."

At the time of the interview, the breach at Carla's restaurant had cost her \$110,000 and counting. "The small business person is taking up the brunt of the whole thing," Carla deplored. "We have to pay for it one way or the other, if not by closing our doors, then by having to pay out big sums of money."



So how do you protect yourself?

Start by educating yourself. The PCI Security Standards Council has developed standards to address the threats to credit card information.

As a restaurant operator, there are two key standards that affect you:



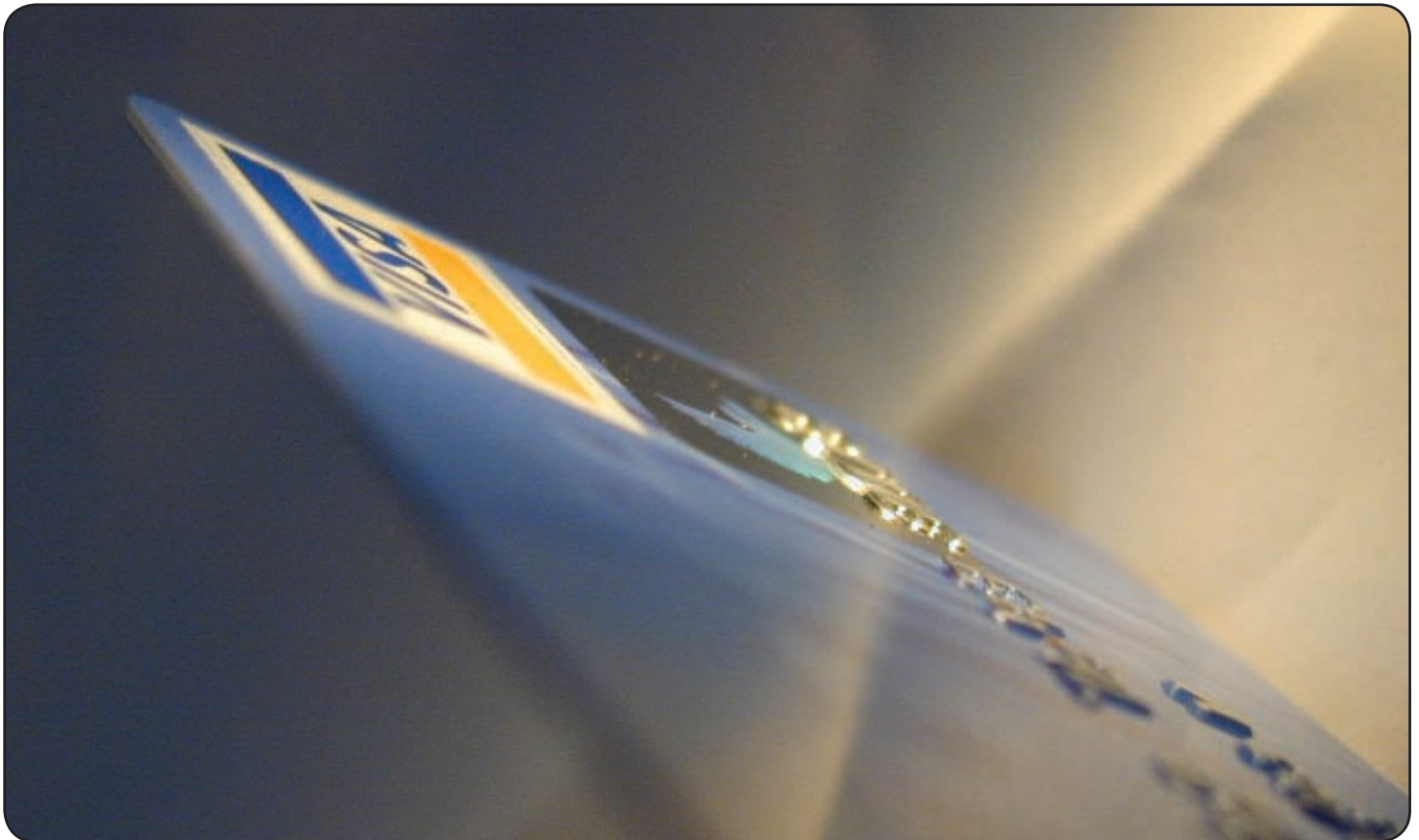
1. The **Payment Card Industry Data Security Standard (PCI-DSS)** outlines the requirements for all merchants that store, process, or transmit cardholder data.

If you process credit cards in your restaurants, you must comply with PCI-DSS.

2. The **Payment Application Data Security Standard (PA-DSS)** covers all software applications used to store, process, or transmit cardholder data as part of authorization or settlement. On October 1, 2008, the PCI Council developed a new standard—PA-DSS—to replace the VISA PABP standard.

PCI-DSS requires that you use only PABP/PA-DSS compliant payment processing and POS systems.

[Check the list of compliant vendors and software.](#)



What are the keys to compliance?

The PCI Data Security Standard outlines 12 key requirements for compliance:

Build and Maintain a Secure Network

- 1: Install and maintain a firewall configuration to protect cardholder data.
- 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

- 3: Protect stored cardholder data
- 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

- 5: Use and regularly update anti-virus software
- 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

- 7: Restrict access to cardholder data by business need-to-know
- 8: Assign a unique ID to each person with computer access
- 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

- 10: Track and monitor all access to network resources and cardholder data
- 11: Regularly test security systems and processes

Maintain an Information Security Policy

- 12: Maintain a policy that addresses information security



Refer to this [great guide](#) put together by the PCI Security Council for more detailed information in an easy-to-follow format.

Ask your POS, credit card processing, and online ordering vendors for copies of their PCI Implementation Guide. All vendors who have been validated compliant are required to provide such a guide.

Find out more

The [PCI Data Security Standard](#) outlines 12 key requirements for compliance.

How does your POS system factor into this?

Your point of sale system is a key factor in safeguarding your business.

One of the most important requirements of the PCI Data Security Standard is the use of point of sale/payment processing software that has been validated compliant.

Why you should care:

The risk to your business in the event of a breach, of course, is the #1 reason to be careful about choosing a PA-DSS validated point of sale application.

But there's another reason, too:

As of July 2010, merchants (including restaurant operators) are required to use only Visa PABP or PA-DSS-validated point of sale and payment applications.



Some financial institutions are already enforcing the requirement for an annual PCI security self-assessment and quarterly network scans—and levying fines for non-compliance. If your POS system is non-compliant after the July 2010 deadline, you will automatically fail your PCI assessment, and could lose the ability to accept credit cards.

If a card data theft is traced back to your business, you are liable. Installing a PA-DSS-validated POS is insurance against this liability. So choose carefully.

Find out more

Learn more about restaurants, credit card security, and PCI:

[National Restaurant Association Briefing: PCI-DSS](#)

[10 Common PCI Myths](#)

PCI Good Business Practices

Protecting your customers' credit card information involves more than just using a PCI-compliant POS. It is important that you also review security management, policies and procedures in your restaurant.

Restrict employee access to your system to what is strictly necessary to accomplish their job. Assign unique IDs and passwords to each user, and ensure old IDs and passwords no longer work.

Restrict access to your router to prevent illicit tampering with your network connections. Keep all terminals in plain sight or under lock and key to prevent illicit use.

You already have safety guidelines for staff. PCI-DSS says you also need to create protective policies for customers' personal information. Likewise, defining IT best practices is really just an extension of your existing operating procedures. Got that covered? Then prepare a maintenance schedule for your POS like the one you follow for your oven to keep up to date.

Add the annual PCI Self-Assessment Questionnaire to your regular insurance review. After all, handling credit card data without the proper controls is like running a business without insurance. Then take a few minutes to schedule your quarterly network scans.



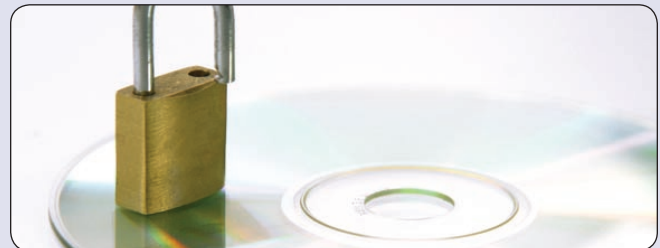
PCI Do's and Don'ts

PCI Do's

- Do routine vulnerability scans of your systems.*
- Do security awareness training for all of your staff.
- Do audits of system access.
- Do monitor your system activity logs.
- Do remove access privileges of separated employees.
- Do install software patches.
- Do take any threats seriously
- Do have an incident response plan in place

PCI Don'ts

- Don't store or archive whole credit card numbers.
- Don't transmit credit card information unencrypted.



Limiting your Liability

It's important to read and understand the **PCI Data Security Standard**, and take the necessary steps to comply.

But limiting your liability ultimately comes down to these five key points:

1. Never...EVER...store cardholder data after transaction authentication.
2. Use a PA-DSS validated POS system.
3. Complete an accurate PCI Self-Assessment Questionnaire each year.
4. Schedule quarterly PCI network scans.
5. Manage your credit card environment like your business depends on it.



Find out more

Go to the source for complete details: [The PCI Security Standards](#)



SpeedLine is the leading provider of intelligent solutions for pizza point of sale. The entire SpeedLine product line has been audited by a third-party security auditor and validated compliant with Visa PA-DSS.

Additional Resources

[Subscribe to the POS Shopping Kit](#)

[Security article](#)

[Loss Prevention article](#)



Tweet this



Share on Facebook



Share on LinkedIn

