Restaurant PCI Basics

PCI is a term that you may have heard every now and then, but may not be overly familiar with. Fear not, because this guide is going to help you understand everything you need to know about the basics of PCI standards and how to keep your restaurant compliant.

SPEEDLINE®

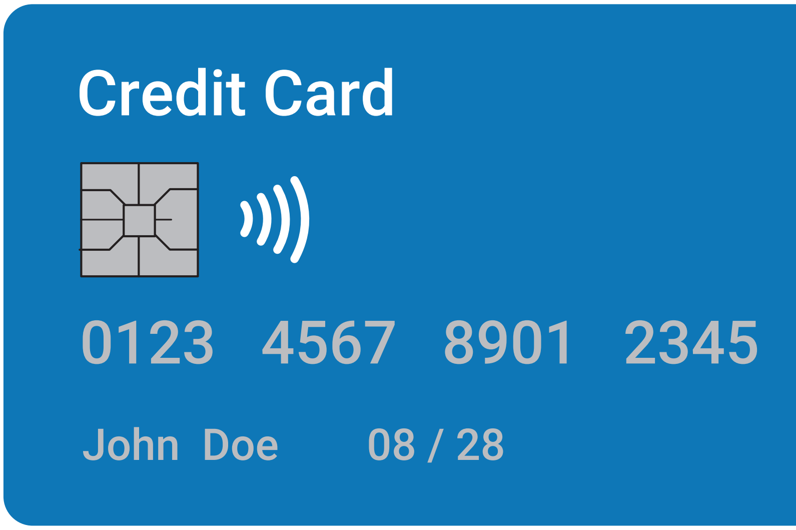
Restaurant PCI Basics

What is PCI?

If you want to better understand PCI compliance, then a good place to start is by defining what the PCI standards are. PCI stands for Payment Card Industry and is a list of standards that are meant to help safeguard customer information while protecting your business.

Compliance with the standards puts a metaphorical lock on your POS system and network, which prevents any unauthorized individuals from accessing your customers' sensitive payment card information. Now, let's put this into perspective, so you can better understand just how important these standards are.

How many orders do you process each day at your restaurant? 200? 300? Maybe more? How many of these are paid for with a credit card? If you're anything like the average QSR restaurant, this number is around 18%, according to Statistica. Once you realize just how many orders this includes, it'll be clear how crucial it is that you protect all of this vulnerable information.

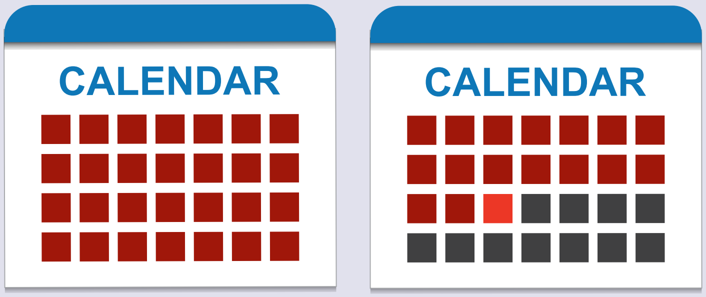


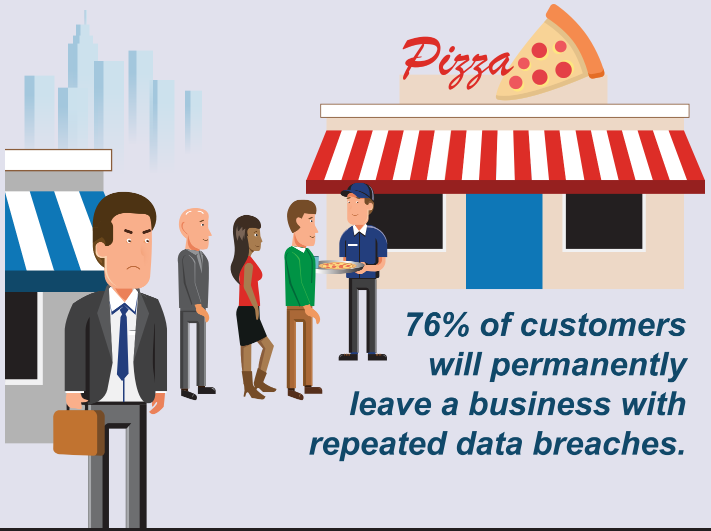
What is the cost of a credit card breach?

If you've never been through a credit card breach before, it can be difficult to understand the high cost associated with it. Between legal fees, security audits, fines, and penalties, it can quickly add up. Not to mention the less tangible (but equally destructive) losses such as brand damage, lost customers, and the man-hours poured into dealing with the breach.

The Bernstein Crisis Management firm reports that the average cost of a breach is $221 for every compromised customer credit card. Depending on how many customers are involved in your data leak, it isn't hard to see how a single breach could cost your restaurant tens of thousands of dollars.

46 days is the average length of time it takes to resolve a data breach.





76% of customers will permanently leave a business with repeated data breaches.

Restaurant PCI Basics

Why Are You Liable for a Credit Card Breach?

Why Are You You know those incredibly long and boring merchant agreements that you signed with Visa or MasterCard? It turns out that by signing those, you became responsible for adhering to the PCI security standards. So if a credit card breach is determined to come from your restaurant, and you aren't fully in compliance with the PCI standards, then you're on the hook for the severe penalties and fines that come along with it.

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

VISA

Rules for Visa Merchants

Card Acceptance and Chargeback Management Guidelines

Small Businesses Are Especially Vulnerable

You might not think that your small restaurant is a particularly interesting target for a data hacker, but Verizon reports that 28% of data breaches happen to small businesses. So it's important to have the right security measures in place, even if you're a tiny mom-and-pop restaurant.

While almost 10% of data breaches happen because the business is using outdated hardware or software, according to Verizon, data mishandling by staff forms a much larger threat. This is responsible for approximately 20% of cardholder data breaches, making it crucial that you and your staff do as much as possible to comply with PCI standards whenever taking a card payment.

Restaurant PCI Basics

Learn the PCI Standards That Affect You

As a restaurant, there are two key standards that are going to impact you:

Payment Card Industry Data Security Standard (PCI-DSS)

This standard outlines the requirements for all merchants that store, process, or transmit cardholder data.

So if you process credit cards in your restaurant, you must comply with PCI-DSS.

Payment Application Data Security Standard (PA-DSS)

This standard covers all software applications used to store, process, or transmit cardholder data as part of an authorization or settlement.

Vendors of payment applications like point of sale systems must comply with this standard.

Restaurant PCI Basics

The 12 Steps to PCI-DSS 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 data.
4. Encrypt transmission of cardholder data across open, public networks.

Maintain a Vulnerability Management Program

5. Protect all systems against malware and regularly update anti-virus software or programs.
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. Identify and authenticate access to system components.
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 for all personnel.

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

Restaurant PCI Basics

PCI Best Practices

Protecting your customers' credit card information involves more than just using a PCI-compliant POS. Here are some other best practices to follow in order to minimize your potential for a data breach.

PCI Best Practices Checklist

- ☑ Restrict employee access to your system to what is strictly necessary to accomplish their job
- ☑ Assign unique IDs and passwords to each employee (or use fingerprint scanners), and ensure old IDs and passwords no longer work
- ☑ Restrict access to your routers to stop anyone from tampering with your network connections
- ☑ Keep all terminals in plain sight or under lock and key to prevent illicit use
- ☑ Create protective policies for customers' personal information
- ☑ Prepare a maintenance schedule for your POS, similar to the one you follow to keep your oven up to date
- ☑ Add the annual PCI Self-Assessment Questionnaire to your regular insurance review
- ☑ Schedule your quarterly network scans
- ☑ Ensure your POS vendors use QIR certified installers

Reducing Your PCI Scope

Although they protect your business, quarterly PCI vulnerability scans and security audits are a significant expense. One way to reduce your PCI scope, and the associated expense, is to use Point-to-Point Encryption (P2PE). In a P2PE setup, certified by the PCI Security Standards Council, payment card information is encrypted by the hardware that reads it, and that information cannot be decrypted until it reaches the card processing software or secure card processing service provider.

EMV PIN pad hardware used with an EMV-capable payment processor that supports P2PE can encrypt payments at the store or at the door. If no payment card information reaches the POS, it will be out of scope for PCI, and there is no possibility of a POS data breach compromising credit card numbers (the rest of your computer network will still require auditing). Processing a chip card with an EMV PIN pad will also give you the best processing rates and protection from chargebacks.

Online, request that your ordering provider send pre-authorized transactions or card tokens to the POS at the store, instead of credit card numbers. Pre-authorizations are preferred, as they include CVV information, which reduces processing rates and protects against chargebacks.

Restaurant PCI Basics

PCI Do's and Don'ts

PCI Do's:

- ✓ Routine vulnerability scans of your systems
- ✓ Security awareness training for all of your staff
- ✓ Audits of system access
- ✓ Monitor your system activity logs
- ✓ Install software patches regularly
- ✓ Take any threats seriously
- ✓ Have an incident response plan in place
- ✓ Read and follow the PA-DSS Implementation Guide for your POS software

PCI Don'ts:

- ✗ Store or archive whole credit card numbers
- ✗ Transmit credit card information unencrypted

PCI Security Standards Council®

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

Find Out More:

☎ 1-888-400-9185 | info@speedlinesolutions.com
www.speedlinesolutions.com

SpeedLine®