The basics of PCI DSS compliance.

Help protect your business by protecting the security of cardholder data and card transactions.

PayPal

Help secure cardholder data by meeting PCI DSS requirements.

One of the biggest challenges for businesses of all sizes is the responsible and secure handling of customer data, sales transactions, and money. Proper handling of this data is a business requirement, and if your efforts fall short, you run the risk of exposing private information should online criminals breach your systems.

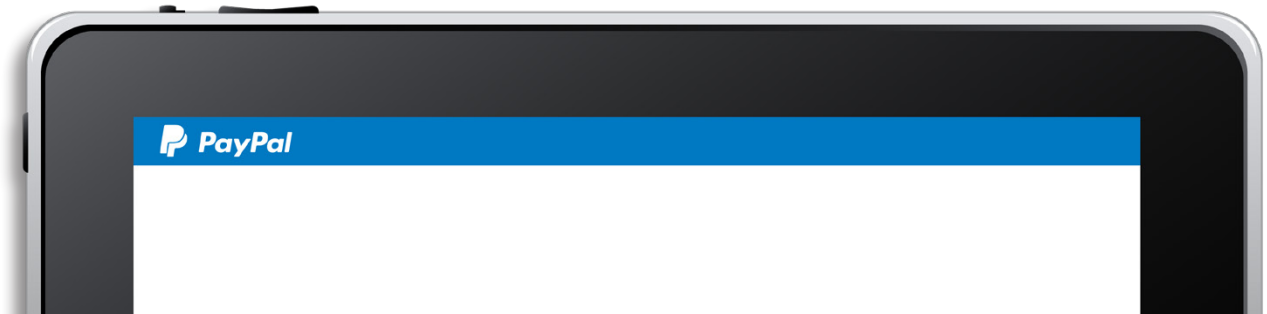
The cost of data breaches can be high. Fraud losses as a portion of merchant revenue were 1.47% in 2016, according to LexisNexis Risk Solutions.* LexisNexis's research also shows that the cost of fraud grew 4 times more in the mobile channel than in the physical point-of-sale channel from 2015 to 2016, which makes security breach prevention all the more important for online merchants. On top of financial losses, businesses can suffer damage to their brand images, since consumers may fear making purchases from a company that can't secure data.

* True Cost of Fraud Study 2016, LexisNexis Risk Solutions, 2016.
** True Cost of Fraud mCommerce 2016. LexisNexis Risk Solutions, 2016.

The Payment Card Industry Data Security Standard (PCI DSS) was created by the payments industry that can help small businesses to protect customer card data located on payment cards. By complying with PCI DSS rules, your business can reduce exposure to fraud and help boost consumer confidence. This guide, which follows the overall goals of PCI DSS, covers the following topics:

- Understanding basic PCI DSS requirements.
- Building and maintaining a secure network.
- Protecting cardholder data as well as data transmissions.
- Maintaining a vulnerability management program.
- Implementing strong access control measures.
- Monitoring and testing networks regularly.
- Maintaining an information security policy.

When you're ready for a deeper dive into PCI DSS, you'll find helpful articles in the PayPal Business Resource Center. For example, you can learn how to choose between hosted and non-hosted solutions to help you comply with PCI DSS.



Your cheat sheet.

PayPal

The basics of PCI DSS.

PayPal

How PCI DSS helps protect your business.

To help businesses reduce risks around data protection and security, the payments industry established the Payment Card Industry Security Standards Council (also known as PCI SSC or the PCI Council) and PCI DSS. The Council and PCI DSS were established and are governed by Visa®, MasterCard®, American Express®, Discover®, and JCB International.

PCI DSS requires any organization worldwide that handles credit card information – including businesses of all sizes, payment processors, and service providers – to follow strict security practices designed to protect customer information.

The PCI DSS requirements apply to all businesses that store, process, or transmit cardholder data. They cover all payment channels, including ecommerce, retail sales at brick-and-mortar locations, and mail and telephone orders.

Penalties for noncompliance can be substantial, and small businesses don't get any leniency – so even if you're just starting out with your business, you need to get serious about PCI DSS compliance. Following PCI DSS requirements offers the added benefit of helping to make sure your infrastructure is secure: the process can help you close any security loopholes in your business, protecting it over the long term.

PCI DSS APPLIES TO ALL PAYMENT CHANNELS.

PCI DSS requirements cover all payment channels, including ecommerce, retail sales at brick-and-mortar locations, and mail and telephone orders.

The more features your payment system has, the more complex it is to secure, whether face-to-face or online.

1. Build and maintain a secure network.

PayPal

Segment cardholder data within your network.

Building a secure network can be more complicated than it seems, since your business is likely using complex, distributed, cloud-based networking to manage customer data and payment transactions. PCI DSS includes 2 specific requirements for building and maintaining a secure network:

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

PCI DSS strongly recommends that any network that handles cardholder data be segmented – that is, kept separate from other systems, such as internal email. The network must also maintain different firewall rule sets and configurations for databases housing credit cardholder information. This can be challenging for a business to manage, even for experienced network administrators.

The same challenges exist for managing passwords of devices such as routers. Use strong passwords and change them often. A strong password has seven or more characters and a combination of upper and lower case letters, numbers, and symbols, like !@#$R&g*.

For more information on password management, check out this PCI DSS infographic.

LET PAYPAL HELP YOU HANDLE DATA SECURITY.

The best way to protect against data breaches is not to store card data at all. PayPal Payments Standard hosts and manages the payment process for you, so customers' card data never touches your company's servers – helping mitigate your PCI DSS compliance requirements.

PayPal is PCI DSS compliant and uses the latest technologies to streamline transactions, while implementing methods to prevent security breaches.

2. Protect cardholder data.

PayPal

Avoid retaining cardholder data.

PCI DSS requirements go into great detail about what constitutes cardholder data and how it must be protected when it leaves your business's networks. Here are the basic rules:

- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.

One of the best strategies to effectively protect cardholder data is to avoid storing it on your networks at all. If you must store it, reduce the number of places where information is stored, limiting the number of points where it can be accessed. The fewer places data is stored, and the less time the data remains in your networks, the lower the risk.

- If you need to keep paper with sensitive data on it, mark through the data with a thick black marker so that it's unreadable, and then secure it in a safe.
- Don't accept payment details via email. Instead, ask customers to provide it via phone, fax, or regular mail.

CONSIDER OUTSOURCING TRANSACTIONS TO KEEP CARDHOLDER DATA OFF OF YOUR SERVERS.

The best strategy for protecting cardholder data is to avoid storing it on your servers:

- **Outsource transactions to a host.** When credit card transactions are processed by a PCI DSS-compliant processor, instead of by your own systems, your compliance burdens are reduced because the card data and transaction never enter your infrastructure.
- **Use a merchant service to process all the transactions.** Because the transaction does not enter your network, the merchant service – not your business – is responsible for meeting PCI DSS requirements.

Encrypt data that travels outside of your networks.

To meet the PCI DSS requirement for encryption, data must be encrypted whenever it travels and wherever it is stored. Encryption technologies can make card data useless even if stolen.

Typically, this requires using strong cryptography, as well as tools to manage encryption keys and keep encryption up to date.

Cryptography uses a mathematical formula to render plain text unreadable to people without a special key.

The PCI DSS rules for data protection also require organizations to develop formal data retention policies. Here's what these policies must do:

- Identify what data needs to be stored.
- Spell out requirements for not storing any data that isn't essential to running your business – such as user authentication codes after authorization is complete, and credit card codes and PINs.
- Specify where data resides so it can be deleted securely as soon as it's no longer needed.

CHOOSE STRONG SECURITY PROTOCOLS.

PCI DSS calls for using strong cryptography to protect sensitive cardholder data during transmission over networks such as the internet, wireless and cellular technologies, and satellite communications.

3. Create a vulnerability management program.

PayPal

Find system weaknesses and repair them.

Whether your business is just getting off the ground or is an established player, you have to worry about your systems' vulnerability to malware, spyware, and computer viruses that could expose customer data. These are the PCI DSS requirements for vulnerability management:

- Use and regularly update anti-virus software or programs.
- Develop and maintain secure systems and applications.

Malware can wreak havoc by taking advantage of vulnerabilities in operating systems and software. Online attackers can gain entry to your data by preying on users (your employees or customers, for example) via the web or through email. Once they find a way in, attackers will look for software vulnerabilities and system misconfigurations to exploit.

PROTECT YOURSELF FROM PHISHING ATTACKS.

Criminals can try to break into your networks via "phishing" – that is, convincing employees and other users to click on an email attachment or link that may contain malware. Educate yourself and your users on how to spot phishing attacks:

- **Avoid mysterious senders.** If you don't know an email's sender, be wary of clicking links contained in a message.
- **Watch for misspellings.** Mistakes in URLs could be signs of a malicious link.
- **Avoid becoming "phish bait."** Be sure to check links you receive in emails by hovering over the link before clicking. If the links don't match, don't click. Also, if you see an IP address (a series of numbers) instead of the usual URL name, that's a red flag.

PayPal

Update and patch software.

Often, software has flaws made by programmers when they wrote the code, also called security holes or vulnerabilities

Hackers exploit these mistakes to break into your computer and steal account data. Protect your systems by applying vendor-supplied "patches" to fix coding errors.

To help prevent online criminals from taking advantage of system and software vulnerabilities, your operating systems and other software must be kept up to date. For example, you should install every software patch available as soon as it's available, as well as anti-malware signatures for any anti-virus software your business is running.

Installing software patches and updates is your best defense against attackers, and the best way to maintain secure systems that house customer data. These updates can help to make your systems more resistant to attacks. For customized software, as well as software developed in-house or by a third party, PCI DSS requires secure development and coding techniques to be in place.

KEEP PATCHING YOUR SYSTEMS.

Install every software patch as soon as it's available. You might get updates from your vendors of your payment terminal, e-commerce host provider, payment gateway, operating systems, and application software.

Make sure to ask ALL your software vendors about how and how often they notify you about patches and updates.

4. Implement strong access control measures.

PayPal

Limit access to cardholder data.

The access control requirements of PCI DSS call for careful management of the people who have access to resources in your business. These are some of the requirements:

- Restrict access to cardholder data on a need-to-know basis – only people who need access to do their jobs should be allowed to view the data.
- Assign a unique ID to each person who has access to places where cardholder data resides.
- Restrict physical access to cardholder data – for example, limiting server access to only those people with special IDs or passcodes.

To comply with PCI DSS, your business should restrict access rights to sensitive data using the fewest privileges necessary for each user's specific job function. You must also document these access controls via written policies, including the specific privileges you're granting to users.

USE TRUSTED BUSINESS PARTNERS.

It's critical to know who your service providers are and how you can get in contact with them. Providers include those who:

- Process your credit and debit card transactions.
- Provide and service your equipment.
- Create applications that support your business activities.

All of these players can impact your ability to protect sensitive customer data, so make sure you learn about their security policies.

See Questions to Ask Your Vendors from the PCI DSS Council.

5. Monitor and test networks regularly.

PayPal

Track access to networks.

Once you implement strong access controls, you're ready to monitor your systems to make sure the controls are working. PCI DSS requirements call for the following actions:

- Tracking all access to network resources and cardholder data.
- Testing security systems and processes regularly.

To stay in compliance with PCI DSS, you must establish processes that track access to system components, and you must create automated audit trails. You'll also need to monitor access to those audit trails, all system logins, and failed login attempts.

Finally, with all of these PCI DSS processes in place – access controls, systems monitoring, vulnerability management, secure coding practices, encryption, and properly segmented networks – make sure that all of these technologies and procedures are running smoothly. Network security controls need to be tested and updated frequently, along with the proper use of network, host, and intrusion-prevention systems.

PROTECT YOUR TRANSACTIONS FROM THE INTERNET.

The internet is the main way that hackers attack and steal customer data. If you're an online seller, make sure you use extra caution to protect your customers:

- Do not surf the web, check emails, or develop your social media marketing campaigns on the same computers you use to process sales transactions.
- Do not attach an external card reader to your virtual terminal. Keep them separate processes.
- If you have a shop and offer free WiFi, make sure you have an entirely separate network to process your transactions.

6. Develop an information security policy.

PayPal

Tell users how to manage cardholder data.

The final section of the PCI DSS requirements contains an important requirement:

- Maintain a policy that addresses information security for employees and contractors.

An effective security policy informs employees of what is expected of them when it comes to protecting cardholder or other sensitive data. The policy also provides your IT department with clear security instructions and objectives.

You'll need to use this written policy to educate people when they're hired, and to remind them of rules on an annual basis. You must also verify that the policy is available to all relevant users, including vendors, contractors, and business partners.

Finally, if cardholder data is shared with service providers, you must create and maintain policies regarding how you manage these relationships and the service providers' access to cardholder data. Also, note that these service providers also will need to be monitored and validated for PCI DSS compliance annually.

THINK ABOUT PCI DSS EVERY DAY.

Creating a security policy isn't just a "set it and forget it" task. You should develop daily operational security procedures that will help employees and partners comply with PCI DSS so everyone knows what's expected of them. To help them understand their roles and responsibilities, your security policy must be available to all relevant users, including vendors, contractors, and business partners – as well as employees.

Learn more about PCI DSS.

At first, PCI DSS compliance may seem to be a difficult challenge for a business. However, given the dangers of data breaches – both the damage to customer safety, as well as the damage to your brand – careful attention to IT security is mandatory. This is a challenge you can meet even if you're a small or medium-sized business. PCI DSS provides the necessary framework so you can protect cardholder data regardless of your size.

Now that you understand the basics of PCI DSS, you're ready to see how PCI DSS compliance standards affect your business. Download the article "PCI DSS Compliance and Your Business" from PayPal's Business Resource Center to understand the approaches and choices that will work best for your business.

Additional resources.

- Visit the PCI Security Standards Council website for a full look at PCI DSS compliance security standards and responsibilities, including training and documents.
- Read the Self-Assessment Questionnaire from the PCI Security Standards Council to identify where you're doing well, and what you need to work on.
- Read the PCI Payment Protection Resources for Small Merchants, an excellent new resource to help small businesses understand the technical and operational requirements of the PCI DSS standards.

PayPal

PAYPAL CAN HELP YOU MANAGE PAYMENT TRANSACTION RISK.

Our merchant services – from all-in-one payment solutions and payment gateways to PayPal Express Checkout – handle data security for transaction processing, helping companies simplify PCI DSS compliance. We process customer debit and credit card information behind the scenes, so card data never touches your servers. That means you have less work to do to prove PCI DSS compliance. For more information about our products, visit www.paypal.com/business.

PLEASE NOTE:

The information in this article has been prepared by PayPal and is for informational and marketing purposes only. It does not constitute legal, financial, business or investment advice of any kind and is not a substitute for qualified professional advice.

You should not act or refrain from acting on the basis of any content included in this article without seeking the appropriate professional advice. The contents of this article contain general information and may not reflect current developments or address your situation. PayPal disclaims all liability for actions you take or fail to take based on any content on this article.

Although the information in this article has been gathered from sources believed to be reliable, no representation is made as to its accuracy. Links and other tools are provided for informational purposes, and PayPal is not responsible for their content. This article is not an endorsement or recommendation of any third-party products or third-party services of any kind.

PayPal