REPAY
Realtime Electronic Payments

Merchant's Guide to PCI Compliance

If you interact with credit card data in any way, you are subject to the PCI DSS standards.

What is PCI?

PCI is a set of standards dictated from the major credit card providers in the market, such as Visa® and Mastercard®, working together to ensure the safety and security of credit and debit card data. The Payment Card Industry Data Security Standard (PCI DSS) is the specific set of requirements designed to ensure that all companies that process, store, or transmit credit card information maintain a secure environment.

What are the Penalties for Non-compliance?

Identity theft is important to all of us. Failing to follow these standards will not only amplify the merchants' risk of data breach and fraud, but failure to adopt and follow the standards may result in severe penalties if a security breach is discovered to be a result of non-compliance. Businesses, and even the owners themselves, failing to comply correctly may be denied the right to process card transactions altogether in addition to the crippling financial burden of fines.

What are the Standards to Achieve Compliance?

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Protect all systems against malware and regularly update anti-virus software
6. Develop and maintain secure systems and applications
7. Regularly test security systems and processes
8. Identify and authenticate access to cardholder data, and restrict overall access
9. Track and monitor all access to network resources and cardholder data
10. Maintain a policy that addresses information security for all personnel

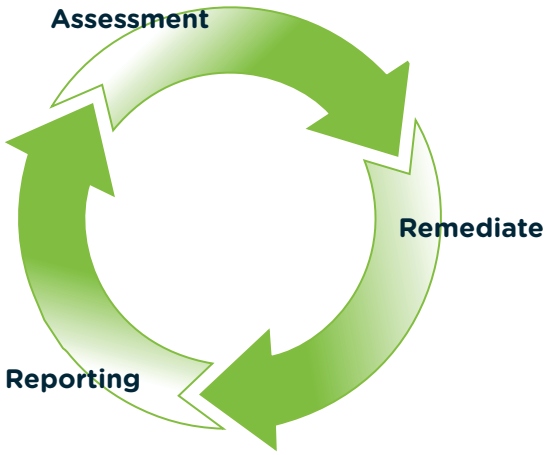
In order to ensure that you have selected a trusted PCI compliant processor, they should provide your business with:

1. Data tokenization
2. Free PCI compliance support
3. PCI-DSS certified gateway for online transactions
4. EMV-certified terminals for card present transactions
5. Automated annual SAQ notification
6. 24/7 live support

PCI Compliance Checklist

Maintaining a safe and secure system is only part of the necessary steps to ensure PCI Compliance. Following January 1st, 2019, all merchants are required to process credit card validations with at least PCI DSS version 3.2.1. Organizations wishing to be compliant and avoid penalties must evaluate their current compliance level, assess their security systems, remediate and fix vulnerabilities, and submit reports and documentation in order to file successfully.

- Before you get started, **contact your merchant bank (acquiring bank)** to check what forms and documentation you will need to submit. The PCI Security Standards Council (PCI SSC) released a new data security evaluation tool that helps assess your PCI DSS compliance and security policy. Some banks may accept this format and others may require you to submit their own evaluation forms.



Assessment: analyze for vulnerabilities
Remediate: fix any vulnerabilities, if found
Reporting: submitting compliance reports and remediation records, where applicable

- **Determine your compliance level** based on how your business is described in PCI general standards so that you are prepared for the following steps. There are different standards for various businesses based on: how you handle customer transactions, how you handle data, what credit card companies and banks you work with, and how much volume you handle.
- Assess your operations as you **fill out the self-assessment questionnaire (SAQ)**. There are nine different versions of the SAQ guidebook, so you will select the one that best applies to your business. The guidebook will walk you through a dozen different requirements for which you'll give a "yes", "no", or "not applicable" answer. This will help you to identify the gaps in your company's payment security.
- At this point, you will know if your business falls short in any way. If this is the case, **make necessary changes** and security improvements to your system. Retake the SAQ to confirm that you are fully compliant.
- **Find a provider that uses data tokenization** to store customers' sensitive credit card information in a secure, web-based portal rather than on your local servers. This will keep their data safe and reduce your liability in the event of a breach.
- Once you have updated your SAQ, you are ready to **complete a formal attestation of compliance (AOC)** - a formal document stating that your business is fully compliant with all relevant PCI standards. A **qualified security assessor** can then review your work and create a report to validate your own findings.
- **File the paperwork** by submitting the documents to your processor and/or acquiring bank. You'll need to submit your SAQ, your AOC, and any other information that your evaluating organizations may request. This may include an external vulnerability scan.

Getting Help

Even though the process for becoming PCI compliant is somewhat straightforward, many technical standards can be confusing if you are not an expert in credit card processing and data security. If you are concerned about your ability to become PCI compliant on your own, it is a good idea to seek help from an outside authority that has expertise in PCI compliance and other data security best practices.

Next Steps

The good news is that REPAY is a 100% PCI-DSS compliant and integrated payment processing solution. We develop, maintain, and support our PCI compliant credit card processing software to ensure that your business is secure and compliant with each transaction. There is no easier way to become PCI compliant than working with the experts at REPAY who will guide you every step of the way.

REPAY (NASDAQ: RPAY) is the premier full-service payment technology and processing provider for a variety of vertical markets. The REPAY payment platform provides direct integration to merchants' core systems and access to a suite of payment technology products. REPAY provides real-time, innovative payment solutions, compliance education, and expertise through exceptional product and service experiences that deliver enhanced value to all stakeholders. With REPAY's integrated omni-channel payment solutions, customers can pay and get paid anytime, anywhere.