

Protecting Customer Data: An Essential Part of Doing Business

What You Need to Know About Payment Card Industry Compliance

Personally identifiable data is everywhere—and everywhere at risk, especially when this data is kept on laptops and other mobile devices. Social security numbers appear in employment and school applications, real estate transactions and medical records. Websites ask for user names and passwords to access content. Credit and debit card information is transmitted over wired and wireless networks, from brick-and-mortar stores and online. Smaller companies, which face particular constraints on time and resources, can be especially vulnerable.

One notable area of concern is credit card data. And it's not just retailers who must be aware of the risks and the required steps to prevent breaches. Anyone who transmits, processes or stores payment card data is at risk—from stores and restaurants to doctor's offices and auto repair shops. In fact, Visa estimates that approximately 85% of data breaches occur at the small business level.¹

Point-of-sale devices, personal computers or servers, wireless networks, Web shopping applications, paper-based and electronic data storage and unsecured transmission of cardholder data to service providers are all vulnerable. On top of that, there may be vulnerabilities in the financial institutions that connect merchants and card payment companies.

Payment Card Industry Compliance: A Security Mandate

To address this growing problem, the major payment card systems, including Visa, MasterCard and American Express, founded the Payment Card Industry (PCI) Security Standards Council and created the Data Security Standard (DSS). Based on industry best practices, this set of 12 comprehensive requirements includes measures to prevent, detect and react to security incidents, and enhance the security of payment accounts. The goal is to make it easier for any business to understand how to safeguard private data and stay ahead of threats to its business and its customers' privacy.

Why Does PCI Compliance Matter to You?

- **PCI compliance is not optional.** It is an industry mandate strictly enforced by the major payment card brands based on the DSS. The DSS applies to everyone who transmits, processes or stores payment card data—regardless of company size or how few card payments it may process. Card payment companies require PCI compliance even if the business processes just a single payment.

¹ <http://www.bbb.org/data-security/intro-to-small-businesses/>



- **Your company's reputation is on the line.** When it comes to a security breach, there is no such thing as good publicity. Stolen data equals stolen trust, and once lost, it may never be recovered.
- **You could be personally liable.** Simply put, you could get sued if your customers' information is stolen. Failing to meet security standards can subject you to potential gross negligence or class-action lawsuits. Your signature on the application to become part of any payment card network means that you become liable if gross negligence can be shown.
- **Fines and penalties can be costly.** If you do not meet PCI compliance requirements, payment card companies may assess steep penalties—up to \$500,000 per incident.¹ They may even stop you from handling credit and debit card payments.
- **It's good business to be safe.** Beyond legal obligations and financial considerations, network security and data protection are an essential part of doing business. By taking the proper steps to protect the privacy and data of your customers, clients or patients, you establish trusting relationships and a positive brand image. True, it costs money to comply. You must pay for infrastructure, technology and time. But just one security breach could cost much more. In short, the cost of compliance is a cost of doing business.

How Can You Ensure PCI Compliance?

Adhere to regulations. In addition to applicable federal and state laws and regulations, businesses that process credit card payments have a responsibility to ensure that they meet the PCI compliance requirements and stay up to date. At a minimum, you must:

- Install a firewall and anti-virus software.
- Make sure patches are up to date.
- Turn off remote access when not needed.
- Change passwords often.
- Stay informed about what is required to maintain compliance.

For example, every time you add a new application or device, you need to take precautions to ensure that it meets security standards and is properly integrated with the rest of your system. A key vulnerability that many business owners may not even be aware of is improperly—or inadvertently—storing cardholder data. Contact your POS provider to see what you're storing on your system.

Ensure that the network is secure and available. Because breaches can still occur after a company passes its audit, you need to:

- Regularly test security systems and processes to make sure they are up to date. Make changes if necessary.
- Maintain an information security policy so all employees are aware of the sensitivity of cardholder data and their responsibilities for protecting it.
- Maintain a plan for responding to incidents.

Enforcement of PCI DSS Compliance

Compliance requirements depend on the number of credit card transactions that are processed per year, with more rigorous monitoring and testing required for businesses that handle more transactions. Businesses are also required to demonstrate ongoing compliance through quarterly testing and an annual assessment. Any company may be audited, whether it processes thousands of transactions or just a few.

Within the PCI Security Standards Council, each payment card company maintains its own compliance enforcement program. Businesses fall into one of four "merchant levels" with any card payment company, based on the number of transactions with that company.



Merchant Levels

Level 1: Any merchant that suffered a breach that compromised its accounts and/or any merchant processing:

- More than 6 million Visa or MasterCard transactions/year
- And/or 2.5 million American Express transactions/year

Level 2: Any merchant processing:

- 1–6 million Visa or MasterCard transactions/year
- And/or 50,000–2.5 million American Express transactions/year

Level 3: Any merchant processing:

- 20,000–1 million Visa or MasterCard e-commerce transactions/year
- And/or fewer than 50,000 American Express transactions/year

Level 4 (Visa and MasterCard only): All others, estimated at more than 5 million businesses

- Up to 20,000 Visa or MasterCard e-commerce transactions/year
- Or up to 1 million Visa or MasterCard transactions/year in all channels

The card payment companies require regular monitoring and testing to ensure that each business remains compliant with the DSS over time. For all levels, network scans are required quarterly by an approved scan vendor (ASV). ASVs are trained and qualified by the PCI Security Standards Council to perform the network and systems scans required by the DSS.

In addition, all but the largest businesses (which must be assessed on-site) are required to complete a self-assessment questionnaire (SAQ) every year. The SAQ includes a series of yes-or-no questions, and “no” answers must include a plan for fixing the problem.

Important Updates

The payment card companies issue new mandates as necessary to help members maintain security as new threats evolve.

- As of April 1, 2010, Visa requires every merchant to be PCI-compliant before accepting Visa card payments.
- MasterCard has redefined its merchant-level categories and deadlines with stricter compliance validation procedures.

PCI compliance is in everyone’s best interest—the payment card company, the merchant or service provider and the consumer. However, it can be difficult for smaller businesses to keep up with new security threats and the industry standards and practices created to address them.

How CenturyLink Business Can Help

CenturyLink Business facilitates compliance by giving customers a single point of contact for all PCI-compliance needs.

Offering an ideal combination of local know-how and personalized service, CenturyLink can help you understand what’s required to achieve and maintain compliance—from basics like installing a firewall and maintaining anti-virus software to identifying what’s stored on your system. We can also help you stay up to date on new technologies and responses to ever-changing threats, helping you to build an effective long-term compliance strategy while making the most of your internal resources.



Data Protection Solutions from CenturyLink Business

CenturyLink Business services include penetration testing, vulnerability assessments, remediation consulting, gap analysis, pre-audit assessments and more. Our solutions, customized to your needs, can help you:

- Stop virus, spam and other dangers from reaching your business.
- Securely transfer data to wherever it's needed.
- Provide reports for auditors and alerts to staff to optimize processes running over the network.
- Provide mobile access to the Internet that offers secure access to your company network via optional VPN client.

PCI Compliance Checklist

Build and Maintain a Secure Network

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

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.

~From the PCI Data Security Standard [Learn More >](#)



Other Resources

Better Business Bureau,
Data Security Made Simpler, 2010

[View pdf >](#)

PCI Security Standards Council,
Data Storage Dos and Don'ts, 2008

[View pdf >](#)

PCI Security Standards Council,
PCI Quick Reference Guide: Understanding the Payment
Card Industry Data Security Standard Version 1.2, 2008

[View pdf >](#)

PCI Security Standards Council,
Skimming Prevention: Overview of
Best Practices for Merchants, 2009

[View pdf >](#)

PCI Security Standards Council,
Ten Common Myths of PCI DSS, 2008

[View pdf >](#)

Protecting Payment Card Data,
CenturyLink Business, 2009

[View pdf >](#)

CenturyLink Service Assurance, 2009

[View pdf >](#)

