

CREDIT CARD DATA SECURITY / PCI COMPLIANCE

PCI DSS:

PCI DSS is a set of technical and operational mandates designed to ensure that all organizations that process, store or transmit credit card information maintain a secure environment and safeguard sensitive credit card data.

Applies to:

PCI compliance applies to ALL organizations, regardless of size or number of transactions, that accept, transmit, or store any cardholder data.

Assurance:

When customers provide their credit cards at point-of-sale systems, over the Internet, on the phone, or through the mail, they want assurance that their account information is safe. These standards were established to provide guidelines to ensure that the best information security practices are implemented and maintained.

Non Compliance:

Failure to comply with the PCI security standards may result in heavy fines, increased processing fees, or suspension of credit card transaction processing services.

Progressive Solutions Helps:

Keeping up with evolving compliance requirements internally is costly and time-consuming. With our hosted solutions, we take on the role of both applications provider and merchant, to help:

- **Mitigate Your Risks** by transferring the storage and processing of credit card data from the city to Progressive Solutions.
- **Reduce Your Costs, Time and Required Resources** for PCI compliance mandates
- **Reduce Your Reporting Requirements** for PCI compliance certification
- **Progressive Solutions** are members of CMRTA, NBBLO, CSMFO and stay apprised of front line issues affecting our customers
- **Progressive Solutions** has provided seminars on data security at these venues for years

How to Comply with PCI DSS

The PCI Security Standards Council sets the standards for PCI security but each payment card brand has its own program for compliance. Specific questions about compliance should be directed to your acquiring financial institution. Links to payment card brand compliance program include:

- **American Express:** www.americanexpress.com/datasecurity
- **Discover Financial Services:** www.discovernetwork.com/resources/data/data_security.html
- **JCB International:** www.jcb-global.com/english/pci/index.html
- **MasterCard Worldwide:** www.mastercard.com/sdp
- **Visa Inc:** www.visa.com/cisp (U.S.)

CREDIT CARD DATA SECURITY / PCI COMPLIANCE

Basic PCI DSS Requirements

PCI DSS consists of 12 Standards with varying levels of requirements depending on the payment card company and the number of transactions processed:

Build and Maintain a Secure Network	<ol style="list-style-type: none"> 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	<ol style="list-style-type: none"> 3. Protect Stored Cardholder Data 4. Encrypt the transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none"> 5. Use regularly updated anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none"> 7. Restrict access to cardholder data to a business need-to know basis 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none"> 10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none"> 12. Maintain a policy that addresses information and data security

Source: PCI Security Standards Council, LLC

CREDIT CARD DATA SECURITY / PCI COMPLIANCE

Ten Common Myths of PCI DSS

Myth 1 – One vendor and product will make us compliant

Many vendors offer an array of software and services for PCI compliance. No single vendor or product, however, fully addresses all 12 requirements of PCI DSS. When marketing focuses on one product's capabilities and excludes positioning these with other requirements of PCI DSS, the resulting perception of a "silver bullet" might lead some to believe that the point product provides "compliance," when it's really implementing just one or a few pieces of the standard. The PCI Security Standards Council urges merchants and processors to avoid focusing on point products for PCI security and compliance. Instead of relying on a single product or vendor, you should implement a holistic security strategy that focuses on the "big picture" related to the intent of PCI DSS requirements.

Myth 2 – Outsourcing card processing makes us compliant

Outsourcing simplifies payment card processing but does not provide automatic compliance. Don't forget to address policies and procedures for cardholder transactions and data processing. Your business must protect cardholder data when you receive it, and process charge backs and refunds. You must also ensure that providers' applications and card payment terminals comply with respective PCI standards and do not store sensitive cardholder data. You should request a certificate of compliance annually from providers.

Myth 3 – PCI compliance is an IT project

The IT staff implements technical and operational aspects of PCI-related systems, but compliance to the payment brand's programs is much more than a "project" with a beginning and end – it's an ongoing process of assessment, remediation and reporting. PCI compliance is a business issue that is best addressed by a multi-disciplinary team. The risks of compromise are financial and reputational, so they affect the whole organization. Be sure your business addresses policies and procedures as they apply to the entire card payment acceptance and processing workflow.

Myth 4 – PCI will make us secure

Successful completion of a system scan or assessment for PCI is but a snapshot in time. Security exploits are non-stop and get stronger every day, which is why PCI compliance efforts must be a continuous process of assessment and remediation to ensure safety of cardholder data.

Myth 5 – PCI is unreasonable; it requires too much

Most aspects of the PCI DSS are already a common best practice for security. The standard also permits the option using compensating controls to meet some requirements. The standard provides significant detail, which benefits merchants and processors by not leaving them to wonder, "Where do I go from here?" This scope and flexibility leads some to view PCI DSS as an effective standard for securing all sensitive information.

Myth 6 – PCI requires us to hire a Qualified Security Assessor

Because most large merchants have complex IT environments, many hire a QSA to glean their specialized value for on-site security assessments required by PCI DSS. The QSA also makes it easier to develop and get approval for a compensating control. However, PCI DSS provides the option of doing an internal assessment with an officer sign-off if your acquirer and/or merchant bank agrees. Mid-sized and smaller merchants may use the Self-Assessment Questionnaire found on the PCI SSC Web site to assess themselves.

Myth 7 – We don't take enough credit cards to be compliant

PCI compliance is required for any business that accepts payment cards – even if the quantity of transactions is just one.

Continued on next page

**PROGRESSIVE[®]
SOLUTIONS**
P.O. Box 783; Brea, CA 92822
Phone: (714) 671 - 1597
Fax: (714) 255 - 9775

Source: PCI Security Standards Council, LLC

Need to contact us?

sales@progressivesolutions.com
support@progressivesolutions.com
webmaster@progressivesolutions.com

CREDIT CARD DATA SECURITY / PCI COMPLIANCE

Ten Common Myths of PCI DSS (continued)

Myth 8 – We completed a SAQ so we're compliant

Technically, this is true for merchants who are not required to do on-site assessments for PCI DSS compliance – for that particular moment in time when the Self-Assessment Questionnaire and associated vulnerability scan (if applicable) is completed. After that moment, only a post breach forensic analysis can prove PCI compliance. But a bad system change can make you non-compliant in an instant. True security of cardholder data requires non-stop assessment and remediation to ensure that likelihood of a breach is kept as low as possible.

Myth 9 – PCI makes us store cardholder data

Both PCI DSS and the payment card brands strongly discourage storage of cardholder data by merchants and processors. There is no need, nor is it allowed, to store data from the magnetic stripe on the back of a payment card. If merchants or processors have a business reason to store front-card information, such as name and account number, PCI DSS requires this data to be encrypted or made otherwise unreadable.

Myth 10 – PCI is too hard

Understanding and implementing the 12 requirements of PCI DSS can seem daunting, especially for merchants without security or a large IT department. However, PCI DSS mostly calls for good, basic security. Even if there was no requirement for PCI compliance, the best practices for security contained in the standard are steps that every business would want to take anyway to protect sensitive data and continuity of operations. There are many products and services available to help meet the requirements for security – and PCI compliance.

When people say PCI is too hard, many really mean to say compliance is not cheap. The business risks and ultimate costs of non-compliance, however, can vastly exceed implementing PCI DSS – such as fines, legal fees, decreases in stock equity, and especially lost business. Implementing PCI DSS should be part of a sound, basic enterprise security strategy, which requires making this activity part of your ongoing business plan and budget.

Source: PCI Security Standards Council, LLC

PAYMENT CARD INDUSTRY SECURITY STANDARDS

Protection of Cardholder Payment Data



**PROGRESSIVE[®]
SOLUTIONS**
P.O. Box 783; Brea, CA 92822
Phone: (714) 671 - 1597
Fax: (714) 255 - 9775

Need to contact us?

sales@progressivesolutions.com
support@progressivesolutions.com
webmaster@progressivesolutions.com

CREDIT CARD DATA SECURITY / PCI COMPLIANCE

Data Storage Do's and Don'ts

Data Do's	Data Don'ts
Do understand where payment card data flows for the entire transaction process	Do not store cardholder data unless it's absolutely necessary
Do verify that your payment card terminals comply with the PCI personal identification number (PIN) entry device (PED) security requirements	Do not store sensitive authentication data contained in the payment card's storage chip or full magnetic stripe, including the printed 3-4 digit card validation code on the front or back of the payment card after authorization
Do verify that your payment applications comply with the Payment Application Data Security Standard (PA-DSS)	Do not have PED terminals print out personally identifiable payment card data; printouts should be truncated or masked
Do retain (if you have a legitimate business need) cardholder data only if authorized, and ensure it's protected	Do not store any payment card data in payment card terminals or other unprotected endpoint devices, such as PCs, laptops or smart phones
Do use strong cryptography to render unreadable cardholder data that you store, and use other layered security technologies to minimize the risk of exploits by criminals	Do not locate servers or other payment card system storage devices outside of a locked, fully secured and access-controlled room
Do ensure that third parties who process your customers' payment cards comply with PCI DSS, PED and/or PA-DSS as applicable. Have clear access and password protection policies	Do not permit any unauthorized people to access stored cardholder data

Please contact **Progressive Solutions** to learn more!