

Payment Card Industry (PCI) Data Security

If You Accept Credit Card Payments, You Need PCI Data Security

The ubiquity of credit/debit cards as consumers' choice method of payment has spawned new opportunities for credit card fraud and identity theft. The proliferation of distribution channels – in-store and virtual – has increased theft opportunity exponentially, and thus, the risk to the consumer. Furthermore, the fragmentation of the payment process across multiple steps and multiple entities (the merchant, the service provider, credit processing entity, hardware platform vendor, etc.) create multiple entry points for thieves to access and misuse customer information.

With each passing day, identity theft and credit fraud are escalating, and this epidemic has the potential to affect all aspects of society. The following table illustrates the pervasive impact of identity theft and credit fraud.

MISUSE OF VICTIM INFORMATION

- Credit Card Fraud – 28%
- Phone or Utilities Fraud – 19%
- Bank Fraud – 18%
- Employment Related Fraud – 13%
- Gov't/Benefits Fraud – 8%
- Loan Fraud – 5%
- Other identity theft – 28%

The payment card industry recognizes the need to mitigate this risk and assure their customers that credit card account information is safe.

To help protect sensitive customer information and maintain consumer confidence, most major credit card associations have adopted the Payment Card Industry (PCI) Data Security Standard, which was jointly developed by VISA and MasterCard.

SAVVIS AND COALFIRE PCI SECURITY SERVICES

- Simplify the PCI process and reach annual deadlines by working with experts in the PCI space
- Rely on trusted partners within the retail space with years of experience serving hundreds of the world's leading retailers
- Choose from annual assessments or on-going assessment services
- Leverage an end-to-end solution that includes PCI assessment, gap remediation and on-going compliance analysis

All merchants and payment processing firms with internal systems that store, process, or transmit cardholder data must comply with the PCI Data Security Standard. For some, self assessment is an option. For high volume merchants and service providers, compliance must be demonstrated by means of an annual assessment conducted by a certified third party assessor.

SAVVIS and Coalfire Systems have teamed to provide the first end-to-end program for PCI. Geared to all merchant and service provider levels, the program is designed to provide a comprehensive solution for both PCI assessment *and* remediation services. Engage the SAVVIS/Coalfire security team to safeguard your customer data and protect your brand integrity.

A Full Service Offering for Cardholder Data Protection

For many merchants and payment processing firms, the introduction of the PCI compliance requirements has resulted in some confusion – What is the requirement for my firm? Where do I turn for assistance? What are the deadlines for compliance and what are the penalties for non-compliance?

If you are a merchant, the first step is to look to your payment processing firm or merchant bank for an understanding of where you fall in the PCI "leveling" – this will impact the steps you need to follow to achieve compliance. There are defined levels for compliance

based upon annual transaction volumes. More detailed information on these levels, compliance requirements and deadlines can be found on the VISA and MasterCard websites.

Depending upon where you fall, self-assessment could be an option, but it is important to evaluate your environment to determine the scope of work that is required. If your organization runs custom applications, maintains a distributed IT environment or uses legacy systems that do not make meeting the PCI requirement straightforward, it may be prudent to engage a third party for assistance. Both MasterCard and VISA provide a list of certified vendors on their respective websites. Choosing the vendor that is right for your organization is an important decision as not all vendors are created equally.

Most assessment programs simply identify areas of non-compliance and leave remediation to your internal staff or to another third party. Additionally, many vendors simply follow the letter of the mandate without applying real world experience in Information Security best practices in order to deliver the most effective security posture possible.

The joint offering from SAVVIS and Coalfire is unique in that it provides a single stopping point for completion of the entire PCI Data Security process – from assessment, to remediation, to on-going compliance analysis. Additionally, our firms deliver more than 35 years of combined experience in the Information Security realm, ensuring that not only the letter of the mandate but the spirit of the mandate will be followed as well.

And, with a broad suite of services that expand far beyond PCI, SAVVIS and Coalfire can easily show your firm how to leverage an investment into PCI to assist with other mandated security programs.

Proven Methodologies Ensure Accurate Results

Both SAVVIS and Coalfire have developed extensive experience with VISA's Cardholder Information Security Program (CISP) and MasterCard's Site Data Protection program (SDP), the precursors to the joint PCI Data Security Standard. As such, we deliver solutions that combine a wealth of experience related to methodologies, tools and templates that drive cost-effective implementation of the PCI standards.

Coalfire is a Qualified Security Assessor and Scanning Vendor for VISA and MasterCard and the Coalfire approach to PCI compliance has been validated by

engagements with numerous merchant and payment processing firms throughout North America.

Coalfire's experience in conducting PCI assessments for very large and complex organizations has provided valuable insight into potential roadblocks and technical issues that may preclude a merchant or service provider from successfully meeting full compliance.

As a result of this experience, Coalfire has developed an approach that consists of both evaluation and consultation. By using this consultative approach, Coalfire can work closely with you to interpret specific requirements and assist in developing solutions that will ensure you fully comply with PCI requirements.

Generally, assessments will be conducted in the following phases:

- Charter and project kickoff
- Data collection and interview
- Data analysis and Report of Compliance (ROC) preparation
- Remediation roadmap documentation
- Management and Engineering presentations and ROC delivery

A Complete Portfolio of PCI Remediation Services

SAVVIS is uniquely qualified to provide PCI remediation services, having worked closely with VISA in developing the components of the original CISP program. As a result of this work, SAVVIS is intimately familiar with the PCI requirements and thoroughly understands their intent and applicability.

Additionally, SAVVIS offers many years of experience in securing the most complex networks of the largest companies in the world, including many of the Fortune 1000 and the United States Government. SAVVIS operates an international security practice with customers in the Finance, Retail, Insurance, Manufacturing and Government sectors. SAVVIS has assisted with regulatory and legal oversight to Congress, the Executive Branch and foreign governments on new security rules and policies. Our engineers have been at the forefront of Information Security and many of them hold advanced technical degrees as well as a wide array of industry-recognized security certifications.

Employing SAVVIS and Coalfire to conduct your PCI



assessment and implement the resulting security enhancements provides valuable assurance that your security posture is consistent with industry recognized best practices and PCI standards.

SAVVIS Remediation Services Include:

- Network Penetration Testing
- Application Code Review
- Security Design & Architecture Services
- Security Policy Design and Deployment
- Managed Intrusion Detection Services
- Managed Application and Content Integrity Monitoring Services
- Managed Firewall Services
- PCI Ready Managed Infrastructure Services

PCI: Complimentary to Other Compliance Mandates

With all of the compliance issues swirling around the industry, PCI may seem to be just another thorn in your side. It isn't. The program will actually improve the management of your business by establishing controls and documenting processes that define your corporate security program. This focus will reduce the amount of time and effort involved with other compliance audits and will enable you to maintain and enhance your security program over time, even if you encounter personnel changes.

SAVVIS and Coalfire recognize that many of the organizations that are required to apply and maintain PCI standards have additional information security initiatives. Our unique approach to PCI will enable your firm to leverage the work done to assist with other mandates such as:

- **Retail Banking:** Gramm-Leach-Bliley Act, FFIEC, USA Patriot Act
- **Retail Drug and Pharmacy:** HIPAA, the Health Alert Network
- **Publicly Owned Organizations:** Sarbanes Oxley Act, ITIL

While PCI compliance may seem like a challenge, not only is it mandatory, it is essential to protect data integrity, customer loyalty and brand integrity.

For more information on this joint offering and to learn how SAVVIS and Coalfire can get you on the path to compliance, contact us today by sending email to retail@savvis.net or contacting us at 1-800-SAVVIS-1