



PAYMENT CARD INDUSTRY (PCI) DATA SECURITY SOLUTIONS

Payment Card Industry (PCI) Data Assessment Solutions

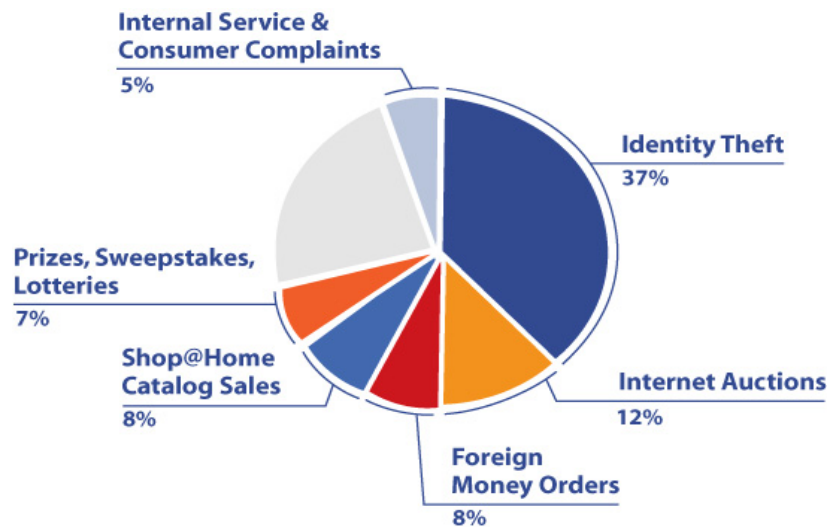
If your organization accepts or processes credit cards, you need PCI Data Security Solutions.

The ubiquity of credit/debit cards as consumers' preferred method of payment for goods and services 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, risk to the consumer. Furthermore, the fragmentation of the payment process across multiple steps and multiple entities (merchants, service providers, credit-processing entities, hardware platform vendors, software providers, etc.) creates multiple entry points for thieves to access and compromise customer information.

With each passing day, identity theft and credit fraud are escalating, and the epidemic is likely to have a direct impact on your organization, if it has not already. The following chart illustrates that identity theft topped the Federal Trade Commission's listing of consumer fraud complaints in the United States for 2005, by a wide margin:

Top Consumer Fraud Complaint Categories

(Reported to the FTC, 2005)



According to the FTC, credit card fraud was the most common form of reported identity theft, trailed by phone/utility fraud, bank fraud and employment fraud. For additional information, including a copy of the complete FTC report, please consult www.ftc.gov. Refer to the press release dated January 25, 2006.

Safeguarding Sensitive Cardholder Information

The Privacy Rights Clearinghouse web site (www.privacyrights.org) has compiled reports of more than 150 data security breaches that occurred from January through August 2006 involving millions of consumer records that contain sensitive personal information. Mindful of the potential risk that results from such breaches, the payment card industry recognizes the need to assure its customers that credit card account information is maintained safely. Specifically, this includes safeguarding information such as customer names, account numbers, expiration dates, billing information, credit limits & spending activity.

PCI SOLUTIONS FROM SAVVIS ENABLE YOUR ORGANIZATION TO:

- Simplify PCI process & achieve annual deadlines by working with experts in the PCI space
- Rely on trusted partners with years of experience in serving hundreds of the world's leading retailers
- Choose from annual assessments or ongoing assessment services
- Leverage end-to-end solutions that include PCI Assessment, Gap Remediation, and ongoing Compliance Analysis

To protect sensitive customer information and to 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. All merchants and payment processing firms with internal systems that store, process, or transmit cardholder data must comply with the PCI Data Security Standard. In certain cases, self-assessment and quarterly network scans may be the only formal requirements. However, for high-volume merchants and service providers, compliance must be demonstrated by means of an annual assessment that is conducted by a certified third-party assessor.

Non-Compliance Penalties

When an organization is found to be in non-compliance, penalties can be severe. In rare instances, merchants or service providers who do not comply with the PCI requirements may be forbidden to store, process or transmit credit card information. Failing to meet required PCI deadlines can result in financial penalties, more stringent audit requirements and possible exclusion from the payment card program. State privacy laws may require public reporting of security breaches that involve customer information, significantly impacting your organization's reputation and brand identity.

When a data security breach takes place, the Ponemon Institute estimates that each "lost" customer record stemming from the breach can result in a total estimated cost to your organization of up to \$140, per customer record. For complete survey results (including the survey methodology), please visit: www.pgp.com/ponemonconsumer.

To facilitate our customers' PCI Compliance activities, SAVVIS has teamed with a Qualified Data Security Company (QDSC) to provide the first end-to-end PCI compliance program, which is geared to all merchant and service provider levels. By engaging the SAVVIS security team, your organization will be able to safeguard customer data and protect your brand identity.

A Full Service Offering for Cardholder Data Protection

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

If you are a merchant, the first step is to look to your payment-processing firm or merchant bank for an understanding of where your organization falls in the PCI "leveling," which will impact the steps you need to follow, in order to achieve compliance. There are defined levels for compliance, based on annual transaction volumes. More detailed information on these levels, compliance requirements and deadlines may be found on the VISA (<http://usa.visa.com>) and MasterCard (<http://sdp.mastercardintl.com>) websites.

Depending on where your organization falls in the "leveling" structure, self-assessment and quarterly network scans could be the only formal requirements. However, it is important to evaluate your environment to determine the scope of work that may be 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 vendor for assistance.

Both MasterCard and VISA provide a list of QDSC vendors on their respective websites. Choosing the vendor that is right for your organization is an important decision, as not all vendors offer the same capabilities.

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

The joint offering from SAVVIS is unique in that it provides a single stopping point for completion of the entire PCI Data Security process – from assessment, to remediation, to ongoing compliance analysis. Additionally, we deliver many years of combined experience in the Information Security realm, ensuring that not only the letter, but also the spirit, of the mandate are followed.

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

BENEFITS OF ONGOING PCI COMPLIANCE

Leverage SAVVIS' Expertise in PCI Compliance

- Protect brand equity & reputation
- Maintain high levels of customer service & efficiency
- Avoid potential loss of revenue due to costly and embarrassing service interruptions
- Keep payment process as efficient as possible
- Maintain customer and investor confidence
- Avoid potential fines, negative press attention, and potential litigation
- Focus corporate attention on importance of ongoing compliance



Proven Methodologies Ensure Accurate Results

Both SAVVIS and SAVVIS' QDSC partner have 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. We deliver solutions that combine a wealth of experience related to methodologies, tools and templates that drive cost-effective implementation of PCI standards. SAVVIS' QDSC partner is a Qualified Payment Application Security Company and an Approved Scanning Vendor for VISA and MasterCard, and its approach to PCI assessment has been validated by engagements with numerous merchant and payment-processing firms throughout North America.

Our partner's experience in conducting PCI assessments for large and complex organizations has provided valuable insight into potential roadblocks and technical issues that may preclude a merchant or service provider from eventually meeting full compliance. As a result of this experience, SAVVIS' QDSC partner has developed an approach that consists of both evaluation and consultation. By utilizing this consultative approach, our QDSC partner will work closely with your organization to interpret specific requirements.

When the assessment process is complete, SAVVIS can assist your organization in developing ongoing solutions that ensure compliance with PCI requirements, going forward. The complete assessment and compliance process consists of eight steps, which are summarized in the chart to the left.

The steps for the complete Assessment & Remediation process include:

- Establish team charter and project kickoff meeting
- Review baseline PCI materials
- Create remediation snapshot
- Prepare high-level data protection assessment
- Develop accessibility assessment
- Prioritize remediation tasks
- Create remediation plan
- Develop supplementary task documents and plan execution

For more detailed information regarding specific tasks that are completed in each of the eight phases, we have also prepared a separate PCI Remediation overview. Please contact your SAVVIS Account Executive for additional details. It is also important to remember that engagements are customized to achieve your organization's goals, and to meet your specific needs.

Maintaining Organizational Security with SAVVIS' Managed Security and Security Consulting Services

This list is a summary of services that are offered separately from the PCI Assessment Service. In some cases, the services are offered solely on servers that are managed by SAVVIS. Since each organization's security environment is unique, please contact your SAVVIS Account Executive for additional details.

SAVVIS Services

In addition to PCI Compliance services, SAVVIS offers a broad range of Managed Security Services and Security Consulting Services to help your organization maintain organizational security.

- Application Security Review
- Assurance Manager
- Content Integrity Monitoring (CIMS)
- Host-based Intrusion Detection (HIDS)
- Incident Response (IR)
- Managed Firewall
- Managed Vulnerability Scanning (MVS)
- Network-based Distributed Denial of Service (DDoS) Mitigation

Applying PCI Knowledge to other Compliance Mandates

With all of the compliance issues swirling around the industry, PCI may seem to be just another in a series of lengthy requirements. It is not. 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 recognizes that many organizations are required to comply with information security compliance requirements that are in addition to the PCI standards. Our unique approach to PCI will enable your firm to leverage our collective experience, 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, it is mandatory, and it is essential to protect data integrity meet customer service expectations and preserve your organization's reputation.

The Next Step in Organizational Compliance

For a brief summary of the current PCI Data Security Standards, see the box below.

Payment Card Industry (PCI) Data Security Standard

Summary of the 12 requirements for PCI Data Security:

Build and Maintain a Secure Network

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

Protect Cardholder Data

3. Protect stored data.
4. Encrypt transmission of cardholder data & sensitive information across 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 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.

Note: These Payment Card Industry (PCI) Data Security Requirements apply to all Members, merchants, and service providers that store, process or transmit cardholder data. Additionally, these security requirements apply to all "system components" which are defined as any network component, server, or application included in, or connected to, the cardholder data environment. Network components, include, but are not limited to, firewalls, switches, routers, wireless access points, network appliances, and other security appliances. Servers include, but are not limited to, web, database, authentication, DNS, mail, proxy, and NTP. Applications include all purchased and custom applications, including internal and external (web) applications.

(Source: VISA Web Site: <http://usa.visa.com>) Important: This summary of the PCI requirements is provided for informational purposes only. Please check the VISA and MasterCard Websites, for the most current information).

About SAVVIS

SAVVIS, Inc. (NASDAQ: SVVS) is a global leader in IT infrastructure services for business applications. With an IT services platform spanning North America, Europe, and Asia, SAVVIS leads the industry in delivering secure, reliable, and scalable hosting, network, and application services. These solutions enable customers to focus on their core business while SAVVIS ensures the quality of their IT systems and operations. SAVVIS' strategic approach combines virtualization technology, a global network and 24 data centers, and automated management and provisioning systems.

For more information about SAVVIS, visit www.savvis.net or call 1-800-SAVVIS-1.