

**June 30, 2010**

**ALERT: Compliance with credit/debit card data security standards required to avoid penalties and maintain ability to accept cards**

If your organization receives, processes or stores data from “payment cards” (credit or debit cards), **you should be aware of and maintaining compliance with the Payment Card Industry Data Security Standard (PCI DSS). Meeting this standard**, created by the Payment Card Industry Security Standards Council to protect consumer data, **is not voluntary**.

**Organizations found to be out of compliance could face penalties or have their ability to accept payment cards revoked** – potentially resulting in significant loss of business, especially for retail establishments. But while PCI DSS compliance can be costly, those expenses pale in comparison to the costs and loss of customers typically associated with a data security breach.

The PCI DSS is a worldwide information security information standard that prescribes specific actions any organization receiving, processing or storing payment card data must take to be in compliance. Five major credit card brands (Visa, MasterCard, American Express, Discover and the Japanese Credit Bureau) originally founded the PCI Security Standards Council, and **all five require organizations using their cards to maintain the PCI DSS or risk losing their privileges to accept those cards**.

The documentation of PCI DSS compliance an organization must provide is based on the volume of payment-card transactions it handles each year, with the highest-volume organizations – or those which have experienced a security breach – required to meet the strictest standards. The highest-volume organizations must not only meet PCI DSS requirements, but also contract for an annual on-site audit of their compliance performed by a Qualified Security Assessor (QSA). Companies with fewer transactions may be able to document compliance through a Self-Assessment Questionnaire.

Broadly, the PCI DSS outlines six goals with 12 related requirements to help an organization develop and maintain a secure data environment as follows:

<b>Goals</b>	<b>PCI DSS requirements</b>
Build and maintain a secure network.	<ul style="list-style-type: none"> <li>• Install and maintain a firewall configuration to protect cardholder data.</li> <li>• Do not use vendor-supplied defaults for system passwords and other security parameters.</li> </ul>
Protect cardholder data.	<ul style="list-style-type: none"> <li>• Protect stored cardholder data.</li> <li>• Encrypt transmission of cardholder data across open, public networks.</li> </ul>
Maintain a vulnerability management program.	<ul style="list-style-type: none"> <li>• Use and regularly update anti-virus software or programs.</li> <li>• Develop and maintain secure systems and applications.</li> </ul>
Implement strong access control measures.	<ul style="list-style-type: none"> <li>• Restrict access to cardholder data by business need-to-know.</li> <li>• Assign a unique ID to each person with computer access.</li> <li>• Restrict physical access to cardholder data.</li> </ul>
Regularly monitor and test networks.	<ul style="list-style-type: none"> <li>• Track and monitor all access to network resources and cardholder data.</li> <li>• Regularly test security systems and processes.</li> </ul>
Maintain an information security policy.	<ul style="list-style-type: none"> <li>• Maintain a policy that addresses information security for employees and contractors.</li> </ul>

The most common reason an organization fails to meet PCI DSS standards is failing to protect stored data adequately; the lack of appropriate, secure storage is also a leading factor in data theft.

PCI DSS requirements periodically change, but the most current information is available through the PCI Security Standards Council's Website at <https://www.pcisecuritystandards.org/index.shtml>.

For more information about how the PCI DSS affects your organization or how to get into and maintain compliance, please contact your AGH professional or AGH's vice president of technology services, Brian Johnson, at (316) 291-4107 or [brian.johnson@aghlc.com](mailto:brian.johnson@aghlc.com).

*NOTE: Information in this document has been obtained by Allen, Gibbs & Houlik, L.C. from sources believed to be reliable. However, AGH does not guarantee the accuracy nor completeness of any information. This communication does not and is not intended to provide advice or counsel, nor is it intended to be used as a substitute for seeking specific advice. Nothing in this can be used to avoid penalties that may be imposed by a governmental authority or agency.*