

PCI Compliance, What in the ?

By Aaron Green, RMCA Vice President

What is PCI and why should you care? PCI stands for Payment Card Industry (PCI) and the full name is Payment Card Industry Data Security Standards or PCI DSS. On July 1, 2010 all merchants or service providers who store, process or transmit customer payment-card data must adhere to information security controls and processes meant to ensure data integrity. This new compliance system will make the *retailer* responsible for fraud. "If there's fraud, then come July 2, the banks will have transferred responsibility over to the dealer or the retailer, and that's the big distinction," Don Churchey, a Sales and Marketing representative for Ewing Oil Co., Hagerstown, Md., told *CSP Daily News*. "The bank is not only going to charge you for what's fraudulent, but they're also going to put a stiff fine on you. They're going to make someone a guinea pig out there."

So how do you find out what to do? Start by visiting the PCI Security Standards Council at <https://www.pcisecuritystandards.org> to begin taking your Self Assessment Questionnaire or SAQ.

According to payment brand rules, all merchants and their service providers are required to comply with the PCI Data Security Standard in its entirety. There are five SAQ Validation categories, shown briefly in the table below. Use the table to gauge which SAQ applies to your organization, then review the detailed descriptions to ensure you meet all the requirements for that SAQ.

SAQ Validation Type	Description	SAQ: V1.2
1	Card-not-present (e-commerce or mail/telephone-order) merchants, all cardholder data functions outsourced. This would never apply to face-to-face merchants.	A
2	Imprint-only merchants with no electronic cardholder data storage	B
3	Stand-alone terminal merchants, no electronic cardholder data storage	B
4	Merchants with POS systems connected to the Internet, no electronic cardholder data storage	C
5	All other merchants (not included in Types 1-4 above) and all service providers defined by a payment brand as eligible to complete an SAQ.	D

Here are some of the basic requirements for all merchants:

- Install firewall protection on all computers
- Do not use vendor supplied passwords
- Protect stored cardholder data
- Encrypt transmission of cardholder data over public networks
- Use and regularly update antivirus software
- Assign a unique ID to each person with computer access
- Regularly test system security and processes
- Maintain a policy that addresses information security

The end result of all of this is that we, the merchant, will be held more responsible for fraud and card information theft than ever before and if it is traced back to your business the fines alone may force you to shut down. Check with your Merchant Services Company and payment Gateway Company to verify that they are PCI Compliant. For more information on specific regulations for each type of card visit these websites:

http://usa.visa.com/merchants/risk_management/cisp.html

<http://www.mastercard.com/us/sdp/merchants/index.html>

<http://www.discovernetwork.com/fraudsecurity/disc.html>

https://www209.americanexpress.com/merchant/singlevoice/dsw/FrontServlet?request_type=dsw&pg_nm=home