



accounting business solutions

May 2010 • Volume 10 • Issue 3

3350A Highway 6, PMB 218
Sugar Land, TX 77478
(281) 652-5947
(281) 596-7273 fax
info@accountingbusinesssolutions.com
www.accountingbusinesssolutions.com

Headline News

Sage Software offers free Web seminars designed to help you better manage your business.

Current offerings include:

- *Critical Compliance: Ensure Your Ability to Accept Credit Card Payments After July 1, 2010.* PCI, PA-DSS, PCI DSS—What does it all mean for your business?

For the current Sage MAS 90 and Sage MAS 200 Webcast schedule or to register [click here](#).



STAR-INFO

Newsletter for Sage MAS 90 and Sage MAS 200 ERP

Payment Card Industry Standards

All Businesses Processing Credit Cards Must Comply

Credit card fraud, fueled in part by the high volume of Web-based credit card transactions, is a serious problem. According to the Privacy Rights Clearinghouse (www.privacyrights.org), more than 100 million records containing sensitive information have been exposed to theft since 2005. The targets are not just large organizations. In fact, smaller organizations with less stringent security measures in place are easy targets for thieves.

Theft typically does not occur during the Internet credit card processing transaction itself—these transactions are well encrypted. Instead, thieves concentrate on breaking into databases that store a large number of credit cards transactions, such as a businesses' accounting system. Regulatory bodies are doing their best to control credit card theft by enacting laws to protect personal information and to regulate the circumstances in which organizations must publicly report a data breach.

Currently, compliance requirements vary according to the number of transactions processed per year. However, regardless of size, organizations processing credit card data must comply with the Payment Card Industry Data Security Standard (PCI DSS). Organizations that suffer a data breach can be fined by their credit card processor if they fail to comply with the standard. Here we provide a brief overview of the PCI DSS requirements.



Data Storage Dos And Dont's

You can store the primary account number, the cardholder name, and expiration date, but this information must be protected per PCI DSS requirements.

You may *not* store the three-digit code on the back of the card, variously called CAV2, CVC2, CVV2, or CID. You also may not store the full magnetic stripe data or PIN information for debit cards.

PCI DSS Requirements

There are 12 components of PCI DSS requirements within the following six categories:

Build And Maintain A Secure Network

(continued on page 2)

Payment Card Industry Standards

(continued from cover)

—The first two requirements relate to the security of a company's network.

1) Install and maintain a firewall configuration to protect cardholder data. A firewall must be present to control the computer traffic between a company's internal network and untrusted external networks. The firewall must examine all network traffic and block transmissions that do not meet specified security criteria—whether entering the system by way of the Internet as e-commerce, employees' access through desktop browsers, employees' e-mail access, dedicated connection such as business-to-business connections, or wireless networks.

2) Do not use vendor-supplied defaults for system passwords and other security parameters. Strong system passwords must be used. The default passwords and settings are well known by the hacker community.

Protect cardholder data—These requirements protect data as it is stored or transmitted.

3) Cardholder data stored in the computer must be protected using programming methods such as encryption, truncation, masking, and hashing. If an intruder gains access to encrypted data, without the proper cryptographic keys, the data is unreadable and unusable to that person.

4) Encrypt transmission of cardholder data across open, public networks.

Vulnerability Management Program—These requirements cover the overall protection of your computer software.

5) Use and regularly update anti-virus software.

6) Develop and maintain secure systems and applications. When a software vendor, such as Microsoft, issues a security patch, it must be installed promptly.

Strong Access Control Measures—The next three requirements relate to access to

information on your computer systems.

7) Restrict access to cardholder data by business need-to-know. Give access to cardholder data only to those who need it to complete their job responsibilities.

8) Assign a unique ID to each person with access to your computer or network. This helps ensure that each individual is uniquely accountable for his or her actions.

9) Restrict physical access to cardholder data. You must secure hard copies of cardholder data in a restricted access location.

Monitor and Test Networks—Even with a well-designed firewall and good anti-virus software, new vulnerabilities are being exposed all the time by malicious individuals. To track and prevent detrimental activity:

10) Track and monitor all access to network resources and cardholder data. You must log user activities so you can detect and track down the cause of a possible data compromise.

11) Regularly test your security systems and processes.

Maintain an Information Security Policy—A strong security policy sets the security tone for the whole company and informs employees and contractors what is expected of them.

12) Maintain a policy that addresses information security.

All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

Sage MAS 90 And PCI DSS

Your Sage MAS 90 and 200 software has been storing credit card data in an encrypted format for some time. With the release of Sage MAS 90 Version 4.4, the encryption algorithms are updated to comply with the latest PCI DSS standards. The update also is being applied in the latest Product Update for

Version 4.3. If you store credit card information in Sage MAS 90 or 200, it is advisable to upgrade to one of these versions as soon as possible to ensure your compliance with the PCI DSS requirements.

The PCI DSS also recommends that if you store credit card transactions, that you periodically purge the data. The Product Update includes a new utility that allows you to safely remove cardholder data periodically, based on a specific transaction or expiration date.

If you are unsure of your compliance in any of the standards, give us a call, or contact your credit card processor. You can visit the PCI Standards Council Web site for more information: www.pcisecuritystandards.org. ✨

((Tips & Tricks))

Filtering Data In Business Insights Explorer Views

You can narrow your result set in a BIE View using any one of the following filtering methods:

- » Click on the value to be filtered, and then click the *Filter by Selection* button on the Business Insights Explorer toolbar. The list is automatically filtered by the selection.
- » Click the drop-down arrow in a column header, and select the value to be filtered from the list. The list is automatically filtered by the selection.
- » Click the drop-down arrow in a column header, and then click *Custom* to open the Custom Filter window. Here you can define either single-level filter equations or groups of equations.

Notes:

- » To remove a filter, click the Remove Filter button on the Data toolbar.
- » Alternate the Data Grid between filtered and unfiltered views by clicking the Toggle Filter button in the Data toolbar.
- » To save a filtered view, click the Save Settings button in the Explorer toolbar.