

Payment Card Industry (PCI) Standards

All Businesses Processing Credit Cards Must Comply

Credit card fraud has been a serious issue for some time now, fueled in part by the high volume of Web-based credit card transactions. The frequency of fraudulent activity continues to grow. According to the Privacy Rights Clearinghouse (www.privacyrights.org), more than 100 million records containing sensitive information have been exposed to theft since 2005, and the targets are not only 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 card 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.

Compliance requirements vary according to the number of transactions processed per year. However, all organizations processing credit card data, regardless of size, must comply with the



Payment Card Industry Data Security Standard (PCI DSS). Organizations suffering a data breach could 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.

Do's And Don'ts Of Data Storage

You can store the primary account

number, the cardholder name, and expiration date, but this information must be protected per PCI DSS requirements—more on that later.

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.

(continued on page 2)

Payment Card Industry Standards

(continued from cover)

12 PCI DSS Requirements

There are 12 components of PCI DSS requirements that fall into the following six main categories. All businesses processing credit cards are required to:

Build And Maintain A Secure Network—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. It 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 should 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) Protect stored cardholder data 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. The particular encryption algorithms that must be used are very specific. Sage MAS 500 has had credit card encryption in place for some time. In Sage MAS 500 Version 7.3, the encryption algorithms have been updated to

meet the new PCI DSS standards.

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 created all the time by malicious individuals. To track and prevent damaging 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 from them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.

12) Maintain a policy that addresses information security.

PCI DSS And Sage MAS 500

Sage MAS 500 Credit Card Processing v7.3 has been tested and verified as being PA DSS compliant. If you store credit card information in Sage MAS 500, it is advisable to upgrade to Version 7.3 as soon as possible to ensure your compliance with PCI DSS. Version 7.3 provides a utility for the safe and secure deletion of historical cardholder data—the new Purge Credit Card Data task. It is your responsibility to remove card validation values or codes and any other credit card data stored in previous versions of Sage MAS 500. The utility also should be used periodically to remove data, based on maintaining a balance between business needs and PCI compliance.

Note: There is no additional charge for the Sage MAS 500 Credit Card Processing module when you use Sage Payment Solutions as the processor.

For additional information on how to implement Sage MAS 500 Version 7.3 in a PCI DSS-compliant manner, see the PA-DSS Implementation Guide for Sage MAS 500 Version 7.3 posted on the Sage MAS Online Community.

If you are unsure of your compliance with any of the other standards, give us a call. ✨

New Sage Product Update Release Format

Sage recently announced some significant changes to the way updates and new capabilities will be delivered to its customers. Sage also announced its plans to retire older versions. These changes are intended to help Sage focus its resources to deliver new functionality faster, as well as give customers ongoing value for their annual subscription plans.

Product Update Delivery

For some time now, Sage has been delivering one major enhancement release every 12 to 18 months. In between, monthly Service Packs have been available for download, to correct any program issues customers might be experiencing. Beginning February 2010, Sage has moved to a Product Update release format. Product Updates will contain a combination of new features and program corrections.

Product Updates will be issued every three to six months, and will be delivered as a downloadable release. The Product Update is intended to provide customers with more value for their maintenance dollars. All product updates are cumulative, so you only need to install the latest product update for Version 7.3. Sage will still correct defects for customers as they occur, and Sage will continue to deliver a major product enhancement release every 12 to 18 months.

Product Retirements

To more efficiently focus development resources, Sage will be reducing the number of versions that it will support. Over the next two years, support this will be scaled back to three versions (current version plus two prior versions). For example, support for Versions 6.3 and 7.0



will end on September 30, 2010. And at the point of the release retirement, 1099 updates, product fixes, and telephone support will end.

First Product Update Available Now

If you currently subscribe to a Sage Business Care plan, the February 2010 Product Updates for Sage MAS 500 Versions 7.2 and 7.3 are available for download from Sage Software Online.

This first Product Update for Sage MAS 500 Version 7.3 includes enhancements designed to make your business processes run more smoothly. Here we provide an overview of the new capabilities:

- **New Security Event for Delete Customer**—To help prevent fraud and protect your sensitive customer information, a new Delete Customer security event has been added for AR Maintain Customers. After installing

the update, as a default all users in the SYSADMIN group will have permission to delete customers. Other users will not be allowed to delete customers. After upgrading, you will want to set this security event as appropriate for your various user groups

- **New Security Event for Changing Sales Order to Quote**—Similar to the delete customer event, another new security event has been added to Sales Order to prevent users from changing a saved sales order to a quote. You can implement this security event for the appropriate users or groups.

- **Sales Order: Warn of Duplicate Customer PO**—To prevent the accidental entry and shipment of a duplicate order to a customer, a new warning message has been added. The message displays in Enter Sales Orders and Quotes if an order or quote is entered with the same customer purchase order number as an order or quote already existing in the database.

- **Warehouse Automation: LabelXpert Sort**—To provide more flexibility in printing labels, a new Sort button has been added in the LabelXpert Pressman to allow a user to sort the grid in a desired order.

Further details on the February 2010 Product Update are available in the Release Notes supplied with the Product Update on Sage Software Online. You will need to login to access the Release Notes. Please call us with your questions about the new Product Update format or the February 2010 Update. ✨

IN THE SPOTLIGHT:

For Your Information — Two Helpful Tips

In this article we cover a couple of common situations customers may experience using Sage MAS 500 ERP and tips for resolving the issues.

Hiding Columns In Business Insights Explorer Views

Business Insights Explorer is a powerful, flexible tool for finding the data you need in Sage MAS 500. However, you may not want all your users to have access to the full power of the tool. There may be a column containing data you would like to keep hidden so that other users cannot view or modify it. You could simply hide the column, but this does not stop another user from modifying the view to expose it again.

To hide a column and prevent users from viewing or adding columns, you must change the mapping. Here we provide an example of removing access to the Sales Territory ID column by mapping it to an incorrect internal column:

1. Expand *System Manager* and *Maintenance*. Double-click *Maintain Business Insights Views / Context Menus*.
2. In the Business Insights View field, select the Customer view.
3. Click the *Column Mapping* tab.
4. In the *View Column* listing, locate the *SalesTerritoryID* row. In the *Permanent Column* list, select *SalesTerritoryKey*.
5. Click the *Save* button on toolbar.

Note: To restore the column, map the View Column to the correct (or matching)

Permanent Column.

You can verify that your mapping was successful as follows:

1. Expand *Business Insights, Explore, and Sales*. Double-click *Customers*.
2. After the customer information loads, verify that the Sales Territory ID column does not display.
3. Verify the column cannot be displayed; on the *Tools* menu, click *Edit Columns* and verify that the Sales Territory column is not listed.
4. Verify the column cannot be used to filter; in the Filter pane, click the *Column* list to confirm Sales Territory is not listed.

Incompatible Database Version

When starting Sage MAS 500 if the version of the database does not match the version of the client software you will receive the following error message: "Sage MAS 500 Client is incompatible with your database version. Please update the appropriate components."

The version of the client software is updated both when a new version is installed, or when components are updated from a Sage MAS 500 service pack or product update. The database version is updated when upgrading the databases, or applying the server portion of a service pack or product update. Sage MAS 500 compares these versions; they must match. This message indicates that either the client or server has been updated, but not both.

If the message indicates a later version of the client, install and run the server portion of the update. To install the server update:

1. Click the *Start* button, point to *Programs*, and *Sage MAS 500*.
2. Click *Sage MAS 500 Server Update*.

If the message indicates a later version of the database, install the client portion of the update on all client workstations. Follow the instructions contained in the release notes or guide accompanying the update.

Please call us with any questions. ✨

CONTACT INFORMATION

ESC Software

1620 W. Fountainhead Parkway
Suite 507

Tempe, AZ 85282

(480) 784-1622

(866) 248-3241 toll free

(480) 784-1623 fax

info@escsoftware.com

www.escsoftware.com

sage

Authorized Partner

Request
More
Information

