



## **Aloha POS v5.3 PA DSS Validation Set to Expire in December, 2009**

Incidences of stolen cardholder account data and system security breaches continue to be a major concern for all participants in the payment industry...and they aren't going away. With the emergence of new threats almost daily, the Payment Card Industry Data Security Standards (PCI DSS) and the Payment Application Data Security Standards (PA DSS) are constantly evolving to ensure cardholder data security.

PCI Data Security Standards state that it is your responsibility, as a merchant, to ensure your system is in compliance with data security requirements. As of December 2, 2009, the PA DSS validation of Aloha<sup>®</sup> POS v5.3 will expire. Radiant Systems, the manufacturer of the Aloha Enterprise suite of products, strongly recommends that you upgrade to the highest Aloha version available.

### **Why you should upgrade....**

- Visa<sup>®</sup> has issued a mandate stating all merchants must be using a PABP or PA DSS validated payment application by July 1, 2010. If the validation of the payment application is expired, the merchant will not be in conformance with this mandate.
- The Payment Card Industry Data Security Standards (PCI DSS) and the Payment Application Data Security Standards (PA DSS) are constantly evolving to ensure cardholder data security.
- Radiant Systems is continuously working on software improvements in each new version of the Aloha Suite to ensure the software meets or exceeds the latest PCI and payment application data security standards.
- Re-validation of older versions does not occur because enhancements are usually required to achieve validation against the new standards.
- A merchant undergoing an assessment by a QSA today may find the experience more intensive and time consuming, and may be found to be non-compliant, if the payment application is not validated based on current data security standards.

To avoid future repercussions for using an expired version of the payment application, contact your Radiant Systems representative today.



## Using Aloha DelTrack to Increase Data Security

The Aloha system meets PCI compliance standards by storing sensitive payment card data in a secure manner; however, the PCI SSC recommends that even secure data be removed when no longer needed. The Aloha DelTrack utility provides a means for increasing data security at the site level by allowing you to remove the encrypted payment card data from stored versions of files in which this data resides.

As you make selections in the DelTrack user interface, the system builds a command line for you, as reflected in the 'DelTrack command line' text box. You can configure the number of recent days to ignore, allowing you to keep a reasonable amount of data on hand based on your data retention policies. You can also include or exclude specific tenders so you can target just your credit card data.

Once the configuration of the command line is complete, you can run the command line using two different methods:

- The most effective method for running the DelTrack command line is copy it into the Winhook batch file so that it runs automatically as part of the End-of-Day (EOD) process. This ensures you are continually removing the encrypted data from the dated subdirectories on a regular schedule.
- You can also create a DelTrack command line to run immediately, either on dated subdirectories in the local %lberdir% file structure, or other locations on the system where you may have copies of dated subdirectories for troubleshooting or other reasons.

Refer to the Aloha DelTrack document for detailed information regarding configuring and using the Aloha DelTrack utility.



## Deadline for Visa Mandates Less Than One Year Away!

The date by which all merchants must meet several Visa® mandates for payment security is less than one year away -----July 1, 2010.

Two of the mandates are part of the initiative for merchants to be compliant with the Visa PIN Security and Key Management Program. This program focuses on “maintaining the highest level of Personal Identification Number (PIN) security.” The third mandate is for merchants to be compliant with the Payment Card Industry Data Security Standards (PCI DSS), which is designed to phase out the use of non-secure payment applications.

| Visa mandate...   | What does this mean to you...   | What happens if you are not compliant by July 1, 2010?   |
|---|---|--|
| All PIN Pads from which you conduct PIN debit transactions must be either VISA PED (PIN-Entry Device) or PCI PED approved.        | You need to ensure you are using only PIN Pad devices that have been either VISA PED or PCI PED approved.   | <p>Visa has not yet published an enforcement plan for using non-Visa PED or PCI PED approved payment devices after this date, but it is probable that some time after July 1, 2010, Visa may begin fining acquiring banks who have merchants using non-Visa PED or PCI PED approved payment devices. These fines will likely get passed on to the merchant.</p> <p>Currently, Radiant Systems supports the following PCI PED approved PIN Pad devices:</p> <p>General Purpose – Verifone 1000SE<br/>           Canadian Debit – Verifone SC 5000<br/>           Aloha Mobile Payment – Verifone V<sup>X</sup>670</p>   |
| Your point-of-sale PIN acceptance devices and host systems must use Triple Data Encryption Standard (TDES).                       | According to the Visa TDES update announced on April 22, 2009, acquirers must develop, and provide to Visa by October 1, 2009, an implementation plan for full TDES compliance for all sponsored activity. The deadline for ensuring all PIN Pad devices use TDES was extended to August 1, 2012. | <p>Per the Visa TDES update, as of August 1, 2012, “Acquirers may be assessed fines for sponsoring any non-TDES compliant merchant.” These fines will likely get passed on to the merchant.</p> <p>The three PIN Pad devices listed above support TDES.</p>  |
| The applications you use for storing, processing, or transmitting cardholder information must be either PA DSS or PABP validated. | You must be using Aloha versions 6.2 and later by the July 1, 2010 compliance date to be in conformance with this mandate.  | <p>Although Visa has not formally published an enforcement plan for non-conformance with this mandate, it is probable acquiring banks that sponsor merchants using non-PA DSS or PABP validated payment applications as of July 1, 2010 will be assessed fines beginning on or after that date. It is also likely these fines will be assessed using the same guidelines for non-conformance to the PCI DSS, which means the fines would be assessed on a monthly basis for each month the merchant is not in compliance. Fines can run anywhere from \$5,000 to \$25,000 per month. Again, These fines will likely get passed on to the merchant.</p> <p><b>Note:</b> The Payment Application Data Security Standards, previously known as Payment Application Best Practices, are standards by which vendors develop their payment applications to help prevent compromises and support overall compliance with the PCI DSS.</p> |

## Deadline for Visa Mandates (cont.)

In addition to the fines assessed by Visa for non-compliance with any one of these mandates, if a security breach occurs and cardholder information is compromised, the merchant is responsible for the cost of the data breach. Recent studies show the cost of a cardholder breach to be around \$125 to \$225 per each compromised record, regardless of whether the data obtained is actually used for fraudulent activity. For example, if data for 2,000 card records is compromised, this security breach could cost as much as \$450,000!

### Are you prepared?

The overall objective of the Visa mandates is to define security measures, agreeable to all, that protect cardholders so that in case you have a security breach, data is not compromised. If you are not already taking steps to be in conformance with the Visa mandates by July 1, 2010, you are putting cardholder data at risk, and also risk incurring sizable fines, as well as the costs related to the security breach.

### Sources:

Visa USA, "PIN Security and Key Management Program" retrieved on 09/22/2009 from [http://usa.visa.com/merchants/risk\\_management/cisp\\_pin\\_security.html](http://usa.visa.com/merchants/risk_management/cisp_pin_security.html)

Visa Business News, April 22, 2009, "Update on Visa's Compliance Policy to Facilitate Triple Data Encryption Standard Usage" retrieved on 09/22/2009 from [http://usa.visa.com/download/merchants/cisp\\_update\\_tdes\\_042209.pdf](http://usa.visa.com/download/merchants/cisp_update_tdes_042209.pdf)

Retail Payments, Friday July 17, 2009, "Visa 7/1/10 Mandate Clarifications" retrieved on 09/22/2009 from <http://retailpayments.blogspot.com/search/label/Visa>



## Buypass/Concord EFS Shutdown Notification

Effective September 15, 2009, First Data withdrew support for the EFSnet platform. As an alternative solution, First Data is providing an emulation service for merchants who use the BuyPass/Concord EFS platform. Aloha customers processing to BuyPass/Concord EFS are not required to make any changes to their software or configurations at this time, as this is being handled by First Data at the processor level.

With the v6.7 release of Aloha EDC in early 2010, a new BuyPass implementation will be provided as a replacement to the current BuyPass/Concord EFS processor. This new implementation will use First Data Secure Transport, formerly known as Datawire, for high speed processing. This update will require Aloha customers to contact their First Data account manager or representative to obtain new merchant configurations for BuyPass. For dialup customers, this may require a phone number update. For high-speed customers, this will require a new host configuration in Aloha EDC.

**Note:** Upon general release of Aloha EDC v6.7, documentation for the new BuyPass implementation will be made available in the EDC Enhancement Release v6.7 document.

### Sources

First Data Corporation, EFSnet Announcement, "EFSnet platform scheduled for 2009 Shutdown" retrieved on 09/23/2009 from <http://www.concordefsnets.com/Home/SunsetEfsnetAnnouncement>.



## National Standard for Menu Labeling and Nutrition Disclosure Being Sought

In a country where obesity in both adults and children is growing at an alarming rate, health experts, restaurant operators, and consumers all agree that nutrition information should be readily available to restaurant guests so they can make more informed food choices when dining out. To assist consumers in making smart food choices, legislation that requires restaurants to disclose nutrition information on their menus and menu boards has been introduced from all levels of government. As a result, there is a maze of legislation that is confusing to both consumers and restaurateurs.

Key sponsors of two competing acts, the Menu Education and Labeling (MEAL) Act (H.R. 3895) and the Labeling Education and Nutrition (LEAN) Act (H.R. 1398), along with representatives of the National Restaurant Association (NRA), and members of the Coalition for Responsible Nutrition Information have been meeting to negotiate an agreement that would clarify and simplify the legislation for the industry while providing consumers the nutrition information they need. As revealed in a Webinar hosted by the NRA on June 26, 2009, they were able to reach an agreement, referred to as the Harkin/Murkowski/Carper negotiated agreement, with compromises being made on each side.

### Four key areas of interest identified by the industry for inclusion in the agreement...

| Area of interest:                       | Industry objective:   | Negotiated agreement:   |
|---|---|---|
| Preemption for state and local mandates | Very important to look for a national solution that would bring uniformity to the requirements across all states, and provide the restaurant industry preemption from state and local menu-labeling mandates.   | The nutrition disclosure legislation is being pursued at the national level and is currently included in the Chairman's Mark on Health Care Reform on the Senate side. It was agreed that should the health care reform bill fail to pass, the negotiated agreement still stands and can easily be moved using other means. |
| Liability protection                    | Wanted to ensure that restaurants who expend the effort to provide detailed nutritional data can do so without fear of liability and frivolous litigation if slight variances exist in the posted information.  | As long as the nutritional data is determined using a "reasonable basis," meaning a nutrient database, cookbook, laboratory analyses, or other reasonable means, the restaurant is in good standing and has a suitable defense for litigation.  |
| Small business protection               | Wanted to ensure the legislation applies to food service establishments that are part of a chain that operates 20 plus units under the same name, independent of ownership. Also wanted to ensure a voluntary program exists for those who wish to have the benefits of this uniformity while the regulators finalize this law. | The voluntary program is available for both those who operate 20 plus locations and those who operate less than 20 locations.   |
| Flexibility                             | Wanted to limit the required nutritional disclosure to calories only; not have it expanded to include other nutritional data, such as carbohydrates, protein, sodium, and more.   | The result of the negotiation was establishments must post the calories for each standard menu item on menus, menu boards, and drive-thru boards, along with the suggested daily caloric intake, and they must state that more detailed nutritional data is available in written format, upon request.                      |

## National Standard for Menu Labeling (cont.)

### Other key points discussed in the NRA Webinar...

- Even though this is federal legislation, it will fall upon state and local health officials to do most of the enforcement, not the U.S. Food and Drug Administration (FDA.)
- Preemption from state and local mandates does not apply until this bill is passed. In the meantime, you must take the necessary steps to comply with state and local laws that are in effect. This does not apply to mandates that have passed but not yet reached their effective dates.
- The legislation for posting nutritional data is not limited to restaurants; it also applies to other venues, such as grocery stores and movie theatres. The 20 plus locations rule also applies to these venues.
- Alcoholic beverages are exempt from this legislation; a few exceptions, mostly items that contain less than 7% alcohol, exist.
- The FDA standard for serving sizes will apply for those items for which the establishment does not control the serving portion, such as a buffet and salad bar.
- A standard menu item is one that is available on the menu beyond 60 days. Disclosures are not required for items on the menu less than 60 days. Items being test marketed extend to 90 days.

This legislation is still in its very early stages, and is currently part of the health care reform bill. Assuming it passes, it will be many months before compliance is required. Once passed, the FDA will address the details for implementing the new legislation. We encourage you to remain aware and educated on this legislation, and to provide input on the regulations when the FDA publishes the proposed rule in the Federal Register for comments from the general public.

### Sources

National Restaurant Association (June 26, 2009) "Menu Labeling Update: What You Need to Know About the New Senate Agreement," retrieved from [http://www.restaurant.org/events/webinars/20090626\\_menu\\_labeling\\_update.cfm](http://www.restaurant.org/events/webinars/20090626_menu_labeling_update.cfm)

GovTrack.us. H.R. 1398--111th Congress (2009-2010): Labeling Education and Nutrition Act of 2009, GovTrack.us (database of federal legislation), accessed on September 19, 2009 from <http://www.govtrack.us/congress/bill.xpd?bill=h111-1398>

Questions or Comments? [ProdMgmt@RadiantSystems.com](mailto:ProdMgmt@RadiantSystems.com)

Acceptance of a given payment application by the PCI Security Standards Council, LLC (PCI SSC) only applies to the specific version of that payment application that was reviewed by a PA-QSA and subsequently accepted by PCI SSC (the "Accepted Version"). If any aspect of a payment application or version thereof is different from that which was reviewed by the PA-QSA and accepted by PCI SSC – even if the different payment application or version (the "Alternate Version") conforms to the basic product description of the Accepted Version – then the Alternate Version should not be considered accepted by PCI SSC, nor promoted as accepted by PCI SSC.

No vendor or other third party may refer to a payment application as "PCI Approved" or "PCI SSC Approved", and no vendor or other third party may otherwise state or imply that PCI SSC has, in whole or part, accepted or approved any aspect of a vendor or its services or payment applications, except to the extent and subject to the terms and restrictions expressly set forth in a written agreement with PCI SSC, or in a PA-DSS letter of acceptance provided by PCI SSC. All other references to PCI SSC's approval or acceptance of a payment application or version thereof are strictly and actively prohibited by PCI SSC.

When granted, PCI SSC acceptance is provided to ensure certain security and operational characteristics important to the achievement of PCI SSC's goals, but such acceptance does not under any circumstances include or imply any endorsement or warranty regarding the payment application vendor or the functionality, quality, or performance of the payment application or any other product or service. PCI SSC does not warrant any products or services provided by third parties. PCI SSC acceptance does not, under any circumstances, include or imply any product warranties from PCI SSC, including, without limitation, any implied warranties of merchantability, fitness for purpose or noninfringement, all of which are expressly disclaimed by PCI SSC. All rights and remedies regarding products and services that have received acceptance from PCI SSC, shall be provided by the party providing such products or services, and not by PCI SSC or any payment brands.

The Compliance Newsletter is published on a quarterly basis. Channel partners can download a copy of each newsletter from the Reseller Portal. Corporate clients can download a copy of each newsletter from the Corporate User Portal. Also refer to the Aloha POS Data Security Handbook, in these same locations, for detailed information regarding configuring an Aloha system to meet PCI requirements.

While the content in this newsletter has been obtained from sources believed to be reliable, no warranty is provided concerning such content and it does not constitute legal advice. Legal advice concerning specific situations should be obtained by your legal counsel.