

Welcome to the July 2007 edition of the Radiant Systems' Compliance newsletter. In May, we launched the first newsletter and have received positive feedback and great comments. We will continue to publish the newsletter bi-monthly. Please feel free to share your comments and questions by emailing them to ProdMgmt@RadiantSystems.com.

American Express CAPN Clarification

In our last newsletter, we announced an extended deadline for CAPN compliance. It is important to note that this extension is only applicable to Aloha merchants who process *direct* to American Express, also known as split dial, using the Aloha EDC program. We agreed on an extended date after a decision to add support for high speed authorization and settlement direct to American Express.



Note: This extension does not apply to merchants processing American Express cards through any other method/processor.

The Balancing Act Over Unused Gift Card Balances

Over the last few years, there has been an explosion of gift card sales within the restaurant industry. Businesses across the country are jumping on the bandwagon to offer customer-enticing electronic gift cards, and why not? The benefits of selling gift cards are overwhelming. Not only do customers enjoy using gift cards, but research shows when customers redeem their gift cards, they tend to spend more than the value of the card. That spells big revenues for restaurants.



Recently, it has also spelled big headaches for restaurants, customers, and legislature, as these three groups are in a conundrum over how best to handle unused gift card balances.

Unused gift card balances are a liability on the books, and can equate to millions of dollars of unrecognized revenue. To solve this issue, some restaurants utilize dormancy fees on unused gift card balances, with the intent to get customers to visit their establishment and use their cards sooner, rather than later or not at all. Aloha eCard is one of many gift card programs that support dormancy fees. The restaurant can determine how much to charge, how frequently, and how long a gift card can go unused before dormancy fees begin.

But customers do not like the fees, which might range anywhere from \$1 to \$2 or more, after a defined period of inactivity. Dormancy fees can cause a \$25 gift card to dwindle down to a zero balance before it's ever used.

Federal and state legislatures also discourage the practice of imposing dormancy fees. The Federal Trade Commission (FTC) is cracking down on what they consider to be cases of inadequate disclosure of dormancy fees and expiration dates to customers. This has prompted some restaurants to rescind their practice of imposing monthly fees on inactive cards, as well as remove expiration dates for gift cards altogether. For those restaurants who elect to use expiration dates and dormancy fees, they must clearly and prominently disclose this information on the gift card. For Aloha eCards, work directly with National Business Products to ensure the policies are clearly indicated on the back of the card.

Laws governing gift cards are different in every state. Some states are passing laws that make the unused balance on a gift card subject to escheat laws, which means the unused balance is treated as abandoned or unclaimed property; therefore, reverting back to the state. Other states have legislature that could be viewed as a win/win for both the restaurant and customer. For example, the State of Illinois passed legislation that would simplify the rules for cards issued in the state by allowing all gift cards issued without an expiration date or dormancy fees to be exempt under the state escheat laws. This means restaurants in Illinois will not miss out on potential profit, since they do not have to turn unused gift card balances over to the state.

Restaurants, customers, and legislation might each have their own idea of how to best handle unused gift card balances. But as this multi-billion-dollar gift card industry continues to grow, all three sides would agree, the need for more straightforward and clear-cut gift card administration practices is greater than ever.

State Gift Card/Gift Certificate Escheat Laws

While abandoned property and escheat laws are different in every state, they can basically be separated into two categories. The first category includes states that specifically exclude gift certificates as part of escheat laws or those states where the law remains ambiguous or unsettled. The second category includes those states that specifically include gift certificates as part of escheat laws or states where gift certificates automatically escheat to the state if they expire before they are used.

States that generally exclude gift certificates as part of escheat laws:

Alabama
Arizona
Colorado (food)
Delaware (less than \$5)
Florida
Idaho (with expiration date)
Illinois (without expiration)
Kansas
Kentucky (unsettled)
Maryland
Massachusetts
Minnesota (unsettled)
Mississippi (unsettled)
Missouri (unsettled)
Nebraska (unsettled)
New Hampshire (under \$101)
New Jersey
New York (unsettled)
North Dakota
Ohio (unsettled)
Oregon
Pennsylvania (unsettled)
Tennessee (no expiration date or dormancy fees)
Texas (food)
Utah (under \$25)
Vermont (unsettled)
Virginia (unsettled)
Wyoming (under \$100)

States that do specifically include gift certificates as part of escheat laws:

Alaska
Arkansas
California
Connecticut
District of Columbia
Georgia
Hawaii
Indiana
Iowa (unsettled)
Louisiana
Maine
Michigan
Montana
Nevada
New Mexico
North Carolina
Oklahoma
Rhode Island
South Carolina
South Dakota
Washington
West Virginia
Wisconsin

(IMPORTANT NOTE: The state information provided here is believed to be accurate as of Jan. 1, 2005. However, no warranty of accuracy is given, particularly since state laws can change frequently. The National Restaurant Association urges you to consult with the relevant state enforcement agency, your legal counsel, and/or your local human resources expert before acting on an important matter related to gift certificates. The information above is provided with the understanding that the National Restaurant Association is not engaged in rendering legal or professional services.)

Jon Hart and Melanie Hill. "Fighting Over the Balance Left on Unused Gift Cards." [The Wall Street Journal Online](http://online.wsj.com/public/resources/documents/SB107219160756934900.htm).
23 December 2003. 12 July 2007 <http://online.wsj.com/public/resources/documents/SB107219160756934900.htm>

"States - Gift Cards/Certificates." [National Restaurant Association: restaurant.org](http://www.restaurant.org/government/state/giftcards/index.cfm). 1 January 2005.
12 July 2007 <http://www.restaurant.org/government/state/giftcards/index.cfm>

For a detailed listing of escheat laws, by state, go to:
http://www.restaurant.org/government/state/giftcards/giftcards_200309_states.pdf

Federal Laws Protecting Consumer Credit Transactions

In response to ever-increasing criminal activities in the area of identity theft, the U.S. Government has initiated the Fair and Accurate Credit Transaction Act, FACTA.



What is FACTA?

The Fair and Accurate Credit Transaction Act of 2003 (FACTA), is a Federal law that gives consumers more rights in the area of fighting the growing crime of identity theft. This law, and its subsequent amendments, gives consumers numerous rights, and also restricts the amount of customer information a printed receipt can contain. FACTA now gives consumers the right to the following, and more:

- Access personal credit files, and to know when the information in them is being used against them.
- Dispute inaccuracies in their credit report.
- Opt out of unsolicited offers.
- Place fraud alerts on their credit reports.
- Block businesses and credit bureaus from reporting information in their credit files that is a result of identity theft.
- Request the exclusion of all but the first five digits of their Social Security number on any reports generated by credit reporting agencies.

FACTA also establishes some requirements that limit how payment card information, and customer information, is displayed. Although hand-recorded or imprint-based receipts are the only exemptions currently permitted, the expectation is that future revisions may address these methods.

- The law requires credit and debit card receipts may not expose more than the last five digits of the account number.
- The law prohibits printing the expiration date.

What does FACTA mean to me?

The significance of FACTA for the community of Aloha users is that you need to be acutely aware of the impact you may have on the ability of the consumer to protect themselves from identity theft. You need to take great care to configure your software systems to prevent storing or printing customer information that someone could obtain and use for illegal activities. Consult the latest version of the 'Aloha CISP Best Practices' document for help with this task.

What happens if a site is not in compliance with FACTA?

FACTA prescribes significant fines for noncompliance with its requirements. Although protecting your customers should be incentive enough for you to comply with FACTA requirements, the fines exist as the punishment side of the equation, to make sure you follow through.

How can I configure a FACTA compliant Aloha POS System?

FACTA compliance for Aloha installations primarily involves preventing customer information from printing or being stored in the POS system. For some areas, specifically the International

market, and for some private label cards, these settings must remain available, as they require this information to print on credit card vouchers.

To configure your Aloha POS system for FACTA compliance:

- Suppress printing the expiration date on vouchers, and all but the last four digits of the payment card number, in Maintenance > Store Settings > Credit Card group > Voucher Printing 2 tab.
- Suppress printing the expiration date on the guest check for the selected payment card tender, in Maintenance > Payments > Tenders > Type tab.

What areas of the federal government are involved with FACTA?

Administering FACTA is a responsibility of the Federal Trade Commission. Issues involving enforcement are the ultimate responsibility of the U.S. Justice department.

Restriction of Hazardous Substances in Electrical and Electronic Equipment

The acronym 'RoHS' stands for "the restriction of the use of certain hazardous substances in electrical and electronic equipment," a directive enacted by the European Union Parliament (EUP). This directive bans selling electronics within the EU



market that contain more than the mandated levels of lead, cadmium, mercury, hexavalent chromium, polybrominated biphenyl (PBB) and polybrominated diphenyl ether (PBDE) flame retardants.

Manufacturers need to understand the requirements of the RoHS directive, to ensure that their products, and their components, comply.

When did RoHS come into force?

The RoHS directive became effective in the EU on 1 July 2006.

Where does RoHS apply?

RoHS is primarily a European standard, but several independent nations and several states in the United States are currently working on their own regulations that are equal to, or more stringent than, the EU RoHS requirements.

What has Radiant Systems done to ensure RoHS compliance?

All new Radiant Systems POS terminal products including the P1220 and P1520 are RoHS compliant, and can therefore be sold in the EU and elsewhere without limitation regarding these regulations. This is important whenever our customers seek to expand or reinvest in their overseas operations, as Radiant Systems can provide them with uniform solutions throughout the world. This capability also maximizes our volumes and efficiencies, helping to keep costs lower for all customers. As laws and regulations change here in the United States, Radiant Systems' customers can be assured that their supplier already has stable and compliant hardware available for sale.

Why should I care about RoHS? What else is Radiant Systems doing?

Although RoHS applies only to product manufacturing today, the possibility exists that amendments to these regulations could eventually include the disposal of older items equivalent to those covered by the primary laws. Legislation in all nations and in the United States is still in flux, so Radiant Systems is paying careful attention to future developments on behalf of our clients. As regulations like RoHS evolve, they may well contribute to an increase in costs for all manufacturers, and therefore some increases in hardware prices. Additionally, it may become more difficult and expensive to dispose of older equipment, regardless of its date of manufacture.

Revision of Access to Aloha Programs



For years, access to Aloha QuickService, TableService, and Aloha EDC has been possible by using the Alt+X key combination, also known as the “super secret password.” However, with the growing threat of identity theft, and the new regulations to combat it, this type of ‘back-door’ access is no longer permissible. Beginning

with Aloha v6.3, the Alt+X entry method is available only if you are using a ‘super-key.’

Why should I upgrade to Aloha v6.3?

Aloha v6.3 incorporates several changes that enhance program security over previous versions, as well as many new features that improve the overall solution. Due to on-going security enhancements released with each new version, it is more important now than ever before to upgrade to the latest versions as they become available.

What methods are you recommending to me for accessing sites?

After upgrading to Aloha v6.3, we recommend the following for accessing your sites:

If you have already implemented ‘best practices,’ unique Back-of-House (BOH) user names and passwords for each site, and if you do not use the Alt-X method of accessing sites, the impact of this change to your operations will be minimal.

If you are accustomed to using remote administration and the Alt-X key combination to log in to Aloha applications, you must revise your method of accessing customer sites. As you develop new methods of supporting your customers, you must exercise great care to avoid compromising your customers’ compliance with PCI (Payment Card Industry) and FACTA (Fair and Accurate Credit Transaction Act) regulations. Resist the temptation to create a single BOH user name and password for use with all of your sites. This method violates PCI regulations, as it creates vulnerability across your entire installed base. Anyone who obtains the user name and password can enter all sites at will. PCI requires each site to have a unique user name with a regularly expiring, ‘strong’ password.

What changes must I make in my operations?

At the highest level, Radiant Systems strives to partner with our customers to do as much as we can to help them be PCI and FACTA compliant. To this end, we have specific recommendations that will help you continue to offer full, rapid support to your sites while maintaining their data integrity.

What do you recommend, prior to upgrading to Aloha v6.3?

Before upgrading your sites to Aloha v6.3 or higher, we recommend you configure a back office security level with full access to all features, with a timeout of 900 seconds or less. Assign this security level to an administrative user at each supported site, and set a different complex password for each administrative user at each site. Use appropriate access controls for the list of administrative users and passwords, to prevent unauthorized site access.

After establishing these security measures, you must perform maintenance on the back office security level with each new version and update, to give the administrative user access to new features, as they become available.

What should I do if I do not have a super key?

We recognize that direct clients and some users will not have super keys. If you do not have access to a super key, work with your support organization to configure access to new features, as they become available.

What should I do if I am using a super key?

If you are using a super key, you can perform the following instructions to maximize access to new features, site by site:

Copy the SECLVLD.dbf and SECLVLDT.dbf files from the site NewData folder to the support office computer, with a super key attached. Make all changes necessary in Back Office Security Levels, and then copy these two files back to the site for subsequent use.

If remote access is not possible, visit the site in person and attach a super key to the file server to make changes, as needed. This process requires you to edit the security key numbers, to make the super key the active key. After service is complete, replace the customer HASP key and restore its numbers to active status. This method gives you direct control over the database and its configuration at each site, with no permanent exposure.

VISANET to Retire the 950 Prefix

If you are a customer who is authorizing or settling credit cards using dialup numbers with a 950 prefix, you need to be aware that these numbers are being retired and will no longer work effective April, 2008. Contact your merchant services department (or bank) to obtain updated phone numbers.



CISP Best Practices Checklist

As you consider a new Aloha installation, you should also include CISP requirements as part of your database building considerations. Here is a checklist that will help you to get an idea of what is involved in CISP compliance:

System Configuration:

Begin configuring your Aloha installation for CISP compliance at the most basic level, initial installation.

- Install the latest CISP validated version of Aloha available.
- After upgrading to a CISP verified version of Aloha, obtain and run the DelTrack utility, to remove any residual customer data remaining in your installation. Refer to the Aloha DelTrack Utility Feature Focus Guide.
- Configure security devices, such as fingerprint scanners, for use on the FOH terminals, when available. Network Security Configuration: Configure your Windows and Aloha networks for security, to give yourself the best chance of retaining data integrity in your installation.
- Verify your Windows installation is set to purge the paging file each time you restart the BOH file server. Information about how to do this is available in the Microsoft Knowledge Base.
- Access the Control Panel, and disable the 'Guest' user. Procedures for doing this vary slightly from one operating system to another.
- Configure data folders relevant to Aloha for access only by the system administrator and other authorized accounts, completely removing the 'Everyone' user from them.
- Install antivirus software, and obtain updates for it routinely and often. Daily is not too often.
- Change all default passwords in routers, remote administrative software, or other third-party hardware or software, as appropriate.
- Install Aloha(QS) in a secondary directory beneath the root, as in D:\Bootdrv\Aloha(QS).
- Ensure procedures are in place to prevent opening a direct Internet connection from any computer on the Aloha network.
- Create a Windows user account specifically for use in the Aloha network, independent of any other network requirements.
- Configure CtlSvr, EDCSvr, RFSSvr, and any other Aloha related services, devices, and BOH user accounts to use the network user account created specifically for this purpose.
- Delete any default Windows user accounts provided by Radiant Systems or affiliated companies for use in initial configuration.

Aloha POS Configuration – Tender Configuration

- Create secure payment card tenders, by suppressing expiration date printing, and by requiring the use of the card itself for transactions, in Maintenance > Payments > Tenders > Type tab.
- Configure Aloha to request the Address Verification System (AVS) security code, if you are using Alohanet, Visanet, BA Merchant Services or RBS Lynk as payment card processors. This setting is in Maintenance > Payments > Tenders > Security Verifications tab.

Aloha POS Configuration – Store Settings:

- Configure printer output to mask the card number and to omit the expiration date, in Maintenance > Store Settings > Credit Card group > Voucher Printing 2 tab.
- Configure Aloha EDC to use an alternate path, outside the BootDrv share, by creating a new environment variable, EDCProcPath, and moving the contents of the current EDC folder to the new location. Refer to AKB ID 8500.
- Require and configure passwords for use on the Front-of-House (FOH) terminals, in Maintenance > Store Settings > Security group > POS Password Settings tab.
- Stop EDC event logging, in Maintenance > Store Settings > System group > Aloha Settings tab.

Aloha POS Configuration – Labor Settings

- Create back office security levels that provide no more access than required for each type of employee, in Maintenance > Labor > Back Office Security Levels.
- Enable the AVS security code override, if you are using one of the processors that request it, in Maintenance > Labor > Access Levels > Financial tab.
- Require each employee to use passwords, and set them to expire regularly, in Maintenance > Labor > Job Codes > Job Code tab.

We recommend you obtain the 'Aloha CISP Best Practices' document, published by Radiant Systems, and use it to compare your current configuration to the recommended practices. This document also contains more detailed information and procedures to help you configure your installation for CISP compliance.

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.



FOR MORE INFORMATION, PLEASE VISIT US AT
WWW.RADIANTSYSTEMS.COM OR CONTACT US AT 877.794.RADS

ATLANTA • DALLAS • LONDON • LOS ANGELES • MELBOURNE • MEMPHIS • PRAGUE • SINGAPORE

CN-HOSP-0607 | © 2007 Radiant Systems, Inc. All rights reserved. Radiant Systems and design is a registered trademark of Radiant Systems, Inc. All other trademarks are the property of their respective owners.

