



MenuLink Enhancements for Amended Hospitality Wage Order in New York

The start of 2011 saw important changes to Hospitality labor requirements in the state of New York. These amended wage regulations took effect January 1, 2011, and cover employees in both the Hotel and Restaurant industries. Radiant Systems is committed to continuously improving features and functionality available for all Aloha Enterprise modules. MenuLink Labor v8.4, scheduled for controlled deployment in late April, was enhanced to use existing Aloha POS data to automate the calculations for the new labor requirements for you.

Recap of the amended labor requirements...

Spread of hours

This regulation states that when the interval between the start and end of an employee's workday exceeds ten hours, he or she is entitled to an additional hour of pay at the basic minimum hourly rate. The span of hours worked begins with the employee's first clock-in and ends with their last clock-out of the business day, including the time they are off for paid and unpaid breaks, as well as other off-duty times, such as between shifts.

For example, if a server works a double shift, with the first shift starting at 11:00 a.m. and the second shift ending at 10:00 p.m., with a three-hour break between shifts, the server is entitled to an extra hour of pay at the basic minimum hourly rate because their workday exceeded the ten-hour "spread-of-hours" limit. Other examples of spread-of-hours greater than 10 are:

7 a.m. - 10:00 a.m., 7:00 p.m. - 10 p.m. = six hours worked but a 15 hour spread.
11:30 a.m. - 3:00 p.m., 4:00 p.m. - 10:00 p.m. = 9 1/2 hours worked but a 10 1/2 hour spread.

The additional hour is not included when calculating overtime, and shall not be offset by any credits for meals or lodging provided to the employee.

Call-in pay

Sometimes referred to as "reporting pay" or "show-up pay," this regulation requires that an employee who shows up to work a regularly scheduled shift or shifts and is sent home early shall be paid at the applicable wage rate:

1. For at least three hours for one shift, or the number of hours in the regularly scheduled shift, whichever is less;
2. For at least six hours for two shifts totaling six hours or less - Receives at least six hours pay, or the number of hours in the regularly scheduled shift, whichever is less; and
3. For at least eight hours for three shifts totaling eight hours or less, or the number of hours in the regularly scheduled shift, whichever is less.

For example, an employee is scheduled to work every Wednesday, from 4:00 p.m. to 10:00 p.m., which is a six-hour shift. The employee reports to work but the manager sends the employee home early, at 6:00 p.m. The employee must be paid for three hours at the basic minimum hourly rate even though they only worked two hours.

A regularly scheduled shift is a fixed, repeating shift that an employee normally works on the same day of each week. If an employee's schedule on a given day of the week changes from week to week, it is not considered a regularly scheduled shift. Payment for actual time worked is calculated at the employee's regular or overtime rate of pay, whichever is applicable, minus any customary and usual tip credit. Payment for the balance of the period is calculated at the basic minimum hourly rate with no tip credit subtracted, and need not be included when calculating overtime.

Employees working in tipped and non-tipped positions on the same day

Some states, including New York, do not allow tip credit when employees work both tipped and non-tipped positions in the same day and the non-tipped hours exceed either a) two or more hours or b) 20% of their daily hours. This regulation states that the employee will be paid at the basic minimum hourly rate for all hours worked that day if either threshold is met.

MenuLink Enhancements (cont.)

For example, an employee works the following schedule:

8 a.m. - 9:45 a.m., preps food;
9:45 a.m. - 1:30 p.m., serves food in the restaurant;
1:30 p.m. – 2:00 p.m. – takes a meal period break;
2:00 p.m. to 4:30 p.m., serves food in the restaurant.

The employee worked a total of 8 hours, 6 hours, 15 minutes in a tipped position, and 1 hour, 45 minutes in a non-tipped position. Twenty percent (20%) of an 8-hour shift is 1 hour, 36 minutes. Although the employee worked for less than two hours in the non-tipped position, this is more than 20% of his/her shift. The employer must adjust the pay rate for the tipped position to the basic minimum wage for each hour worked in that position.

Click [here](#) to read more about the new mandates.

PABP v1.4 Extended Deadline Has Passed

The extended deadline of March 2, 2011 for payment applications validated using Payment Application Best Practices (PABP) v1.4 has passed...

How does this impact organizations currently using Aloha POS v6.2?

Aloha POS v6.2 was validated using PABP v1.4, so as of March 2nd, this version is no longer acceptable for new installations; however, POS v6.2 is acceptable for pre-existing installations, as long as the following remains true:

- Radiant Systems is still providing software support for Aloha POS v6.2.
- The site is on software maintenance, which entitles them to patches and upgrades.



It is expected that Aloha POS v6.2 will be retired as of June 1, 2011.

- The site implements all critical patches and updates within 30 days of the release.

As a reminder, the following Radiant POS applications are currently listed on the PCI DSS List of Validated Payment Applications as acceptable for new deployments:

Version number	Validated against PABP/PA DSS version:	Current validation expires on:
Aloha POS v6.4*	PA DSS v1.2	October 2, 2013
Aloha POS v6.5	PA DSS v1.2	October 2, 2013
Aloha POS v6.7	PA DSS v1.2	October 2, 2013
Aloha Takeout v1.2	PA DSS v1.2	October 2, 2013

*Radiant Systems will retire Aloha POS v6.4 when Aloha POS v7.0 reaches market-ready status.

The following versions remain on the list of validated payment applications, but are acceptable only for pre-existing installations:

Version number	Validated against PABP/PA DSS version:	Current validation expired on:
Aloha POS v5.3.15	Prior to PABP v1.3	December 2, 2009
Aloha POS v6.1	PABP v1.3	June 2, 2010
Aloha POS v6.2	PABP v1.4	March 2, 2011
Aloha Takeout v1.1	PABP v1.4	March 2, 2011

Access the following Web site to view the list of validated payment applications, and their expiration dates, as published by the PCS SSC:

https://www.pcisecuritystandards.org/approved_companies_providers/index.php





Update: Card Brand Mandates

Radiant Systems has published several communications outlining the requirements and dates by which you must comply with mandates issued by the MasterCard and Discover credit card brands. This communication includes changes to the message and should also serve as a reminder of the upcoming deadlines.

What's new with this communication?

We have simplified our message on the mandates, and the minimum required software versions may have changed based on new information from the two major card brands and several processors. Please use the sections below to determine the versions you will need.

Detailed information about the MasterCard requirements

MasterCard has issued requirements for real-time reversal and partial authorization support, for which most processors are stating you have until November, 2011 to make the changes required to support the mandates.*

Partial Approvals – MasterCard requires partial authorization support for prepaid credit and debit cards, with balance response, if available. This support allows a merchant to authorize a portion of the original transaction amount, if the transaction amount exceeds the available balance on the card. Guests can use the remaining balance of a prepaid card as partial payment of a transaction without the risk of being declined, and pay the balance of the transaction using an alternate form of payment.

Real-Time Reversal – MasterCard requires real-time reversal (void) support for credit and debit card authorizations, to prevent delays in guests regaining access to their funds when a sale is not completed. The current process of providing cash back when a debit void cannot be performed meets this requirement.

To support the MasterCard requirements...		
Credit card acceptance only		
Minimum Aloha POS v6.5	Minimum Aloha EDC v7.0	Available in Q2, 2011
Credit card and PIN debit acceptance		
Minimum Aloha POS v7.0	Minimum Aloha EDC v7.0	Available in Q2, 2011

*Please note, Fifth Third Bank is requiring merchants to make the necessary changes to support the MasterCard mandates by May, 2011.

Detailed information about the Discover requirement

Discover recommends that you always enter the Card Identification Number (CID) for transactions when manually entering the credit card number. The CID is a three-digit security code printed on the back of the card. Requiring the entry of this code helps validate the legitimacy of the card, thus reducing fraud.

Discover has indicated it is at the discretion of your processor as to whether you need to support CID entry for manually entered card numbers. Communicate directly with your processor to determine if you need to support CID entry, and the date by which you must be able to support it. *

To support the Discover requirement...		
CID entry for manually entered Discover cards		
Minimum Aloha POS v6.7	Minimum Aloha EDC v7.0	Available in Q2, 2011

*In addition, some processors may request you enter a reason when a CID is not entered. We added this newest enhancement in Aloha POS v7.0 and Aloha EDC v7.0. Refer to the Aloha EDC v7.0 Enhancement Release document for how to configure this functionality.

To configure Aloha Manager v6.7 to require the entry of the CID:

1. Select **Maintenance > Payments > Tenders**.
2. Select a **credit card** from the drop-down list.
3. Select the **Identification** tab.
4. Select **Require Identification** to enable the options on the Security Verifications tab.
5. Select the **Security Verifications** tab.

Card Brand Mandates (cont.)

6. In the **Validation Code** group box, select the following:
 - **Enter Validation Code** – Select this option to enable validation code entry.
 - **Required** – Select this option to enforce the entry of the CID even when a manager, or employee with sufficient access, approves the omission of the validation code. To allow certain employees the ability to bypass the CID prompt, select 'Override Security Verification' in the access level to which they are assigned.
 - **All Cards** – Select this option to require the entry of the validation code for all transactions, even if the card number was not entered manually on the FOH.
 - **Numeric entry only** – Select this to limit the data you can enter to numeric values only.
 - **Prompt twice** – Select this option to require the entry of two matching validation codes before you can proceed (Not recommended).
7. Select the **minimum** and **maximum** number of digits to enter, typically three.
8. Type the **text to prompt** for the validation code on the FOH Security Verification screen. You can type up to 20 characters, e.g., 'Validation Code.'
9. Click **Save** and exit the **Tenders** function.

Key Licensing Requirements for Aloha EDC v7.0

Good news! Effective with the release of Aloha EDC v7.0, available in Q2, 2011, you will not be required to upgrade the version that is licensed on the security key. Please note that in earlier communications, we indicated Aloha EDC v6.9 was a viable option for select processors; however, we made important changes in Aloha EDC v7.0, and we will not be generally releasing Aloha EDC v6.9.

If you have any questions about this communication, please contact your Radiant Systems representative.



Voluntary Use of Fingerprinting Devices in New York is Permissible

Biometrics technology uses distinctive physiological and behavioral characteristics to authenticate someone is who they say they are. There are several forms of biometrics technology, including fingerprints, retinal scans, and hand-writing, but fingerprint-based biometrics is the most commonly used form. As biometrics technology continues to advance and the risks associated with fraudulent access to computer networks continues to increase, companies are looking to this technology to provide more robust security, particularly as it relates to employee "identification." Because every individual has a unique fingerprint, companies are implementing the use of fingerprint scanners, in lieu of employee badges, which are easily lost or stolen, to ensure the person logging in to the computer is really who they say they are.

Concern over whether the use of biometrics technology for the purposes of logging in to a computer violates an individual's privacy has been raised, and some states are intervening, such as the state of New York. Section 201-A of the New York Labor Law states that fingerprinting of employees is prohibited, unless otherwise provided by law. It goes on to say that no person, as a condition of securing employment or of continuing employment, shall be required to be fingerprinted.

Does the use of a "fingerprinting" device for time clock purposes violate Section 201-A of the New York Labor Law?

In an opinion issued by a representative of the New York State Department of Labor in April, 2010, the representative clarifies Section 201-A of the labor law. In summary, the opinion states that:

A biometric scan is similar or comparable to the scanning of a fingerprint; therefore, an employer may not require its employees to use the biometric device for the purposes of clocking in.

The opinion goes on to say voluntary fingerprinting of employees is not prohibited by the labor law; however, employers cannot coerce employees to participate in the fingerprinting program, and no "adverse employment action" can be taken against employees for not volunteering to participate in the fingerprinting program.

Voluntary Use of Fingerprinting Devices (cont.)

Aloha POS software supports multiple login features, including voluntary biometric login.

The Aloha POS software provides multiple login options at the employee level, including employee number and password, magnetic card swipe, and biometric login.

Radiant Systems provides several point-of-sale terminals that support the use of slide fingerprint scanners, designed for reading fingerprint patterns as the finger slides across the scanner. The majority of these scanners are manufactured by AuthenTec, Inc., or UPEK, and work quickly and with great accuracy.

To configure the “voluntary” use of the fingerprint scanner for clocking in, and subsequently logging in, access the appropriate employee record in Employee Maintenance and select:

- Must use Fingerprint Scanner – Clock In
- Must use Fingerprint Scanner – Log In/JIT

If an employee chooses not to use the fingerprint scanner, you may select “Must use Mag Card” instead, and then click Mag Card Password to assign a mag card to the employee.

When using a fingerprint scanner, you must first “enroll” the employee into the system. The employee will slide their finger across the scanner several times during the enrollment process; however, biometrics technology does not actually capture and store the fingerprint. Instead, it uses a mathematical algorithm to record the pattern of “landmarks” in a fingerprint. After a successful enrollment, when an employee slides their finger across the fingerprint scanner, the system compares the new scan to the stored pattern, and access to the computer is achieved when a match is found.

Questions or Comments? 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.