

by Linda Carter
© The Retail Management Advisors, Inc.
email: LC@the-retail-advisor.com

~~~~~  
**May 15, 2010**  
~~~~~  
in this issue . . .

- **NEW FOR 2010: TAX CREDIT HELPS SMALL EMPLOYERS PROVIDE HEALTH INSURANCE COVERAGE**
- **COMPUTER SECURITY - PCI COMPLIANCE**
- **WHAT IS THE CORRECT WAY TO CALCULATE MARKDOWN % ?**
- **QUOTE OF THE MONTH**
- **INTERNAL CONTROL MANUAL**
- **OPEN-TO-BUY**
- **WHAT WE DO . . .**

NEW FOR 2010: TAX CREDIT HELPS SMALL EMPLOYERS PROVIDE HEALTH INSURANCE COVERAGE

~~~~~  
IR-2010-38, April 1, 2010

WASHINGTON — Many small businesses and tax-exempt organizations that provide health insurance coverage to their employees now qualify for a special tax credit, according to the Internal Revenue Service.

Included in the health care reform legislation, the Patient Protection and Affordable Care Act, approved by Congress and signed by President Obama on March 23, the credit is designed to encourage small employers to offer health insurance coverage for the first time or maintain coverage they already have. In general, the credit is available to small employers that pay at least half the cost of single coverage for their employees.

“This credit provides a real boost to eligible small businesses by helping them afford health coverage for their employees,” said IRS Commissioner Doug Shulman. “We urge small businesses and tax-exempt employers to look closely at this important tax break — which is already effective — to see if they qualify.”

The maximum credit is 35 percent of premiums paid in 2010 by eligible small business employers and 25 percent of premiums paid by eligible employers that are tax-exempt organizations. In 2014, this maximum credit increases to 50 percent of premiums paid by eligible small business employers and 35 percent of premiums paid by eligible employers that are tax-exempt organizations.

The credit is specifically targeted to help small businesses and tax-exempt organizations that primarily employ low and moderate income workers. It is generally available to employers that have fewer than 25 full-time equivalent (FTE) employees paying wages averaging less than \$50,000 per employee per year. Because the eligibility formula is based in part on the number of FTEs, not the number of employees, many businesses will qualify even if they employ more than 25 individual workers.

The maximum credit goes to smaller employers — those with 10 or fewer FTEs — paying annual average wages of \$25,000 or less.

Eligible small businesses can claim the credit as part of the general business credit starting with the 2010 income tax return they file in 2011. However, an employer you need to show a profit and tax liability to claim the tax credit. The credit for a year offsets only an employer's actual income tax liability (or alternative minimum tax liability) for the year. However, as a general business credit, an unused credit amount can generally be carried back one year and carried forward 20 years. Because an unused credit amount cannot be carried back to a year before the effective date of the credit, though, an unused credit amount for 2010 can only be carried forward.

The IRS will use postcards to reach out to millions of small businesses that may qualify for the credit. The postcards will encourage small business owners to take advantage of the credit if they qualify.

More information can be found on the web at:

<http://www.irs.gov/newsroom/article/0,,id=220839,00.html>,

[http://www.irs.gov/pub/irs-utl/3\\_simple\\_steps.pdf](http://www.irs.gov/pub/irs-utl/3_simple_steps.pdf) or

<http://www.irs.gov/newsroom/article/0,,id=220809,00.html>.

## COMPUTER SECURITY - PCI COMPLIANCE

~~~~~

An optimistic outlook may be the simplest single explanation for data security breaches. To often, management has the outlook of, "Yes, I know it happened to **them**, but it won't happen to us." In a 2006 article for the Pittsburg Post Gazette, writer Sasha Romanosky wrote that "optimism bias encourages a state of denial" and those merchants who don't recognize that fact are putting their most vital information at risk.

Since data breaches continue to be an ever increasing problem, the PCI Security Standards Council, comprised of representatives from American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc. International, have developed the PCI compliance standards comprised of principles and requirements to support those principles with the goal of helping ensure consistent data security measures on a global basis.

What is PCI compliance?

The **P**ayment **C**ard **I**ndustry **D**ata **S**ecurity **S**tandard (PCI DSS) is a set of requirements designed to ensure that **ALL** companies that **process, store or transmit** credit card information maintain a secure environment for that information. Compliance is not a federal law. Many states do have laws requiring some level of PCI compliance. When considering requirements of PCI compliance, keep in mind having a lock on your front door is not a law . . . it's just common sense to protect what's yours.

Who does PCI compliance effect?

PCI compliance affects anyone with a **merchant id number without regard to the number of transactions or sales volume**. Some state laws do not compel Level 4 Merchants (those completing fewer than 20,000 transactions annually) to comply; however, more and more states require notifications to customers who may have been affected when a data breach occurs. Think of the potential harm of this type of negative publicity not to mention the civil suits sure to follow.

Requirements of PCI

Stop and think about computer security. If you are ordering postage stamps or office supplies on your computer, you expect **those vendors** to have a secure method to process your credit card number and accept and process your order. It is only logical that **you** also need to have a secure environment (your store's computer system) to **send** that information to them. The PCI requirements are not unusual and what many Americans already have in place at their homes for their leisure web-surfing and personal email. ***It is just plain common sense*** like the lock on the door.

The core of the PCI DSS is a group of principles and accompanying requirements around which the specific elements of recommended security are organized:

Principle	Requirement
Build and Maintain a Secure Network	<ul style="list-style-type: none"> ▶ Install & maintain a firewall ▶ Do not use vendor supplied defaults for passwords and other security parameters.
Protect Cardholder Data	<ul style="list-style-type: none"> ▶ Protect stored cardholder data ▶ Encrypt transmission of data.
Maintain a vulnerability management program	<ul style="list-style-type: none"> ▶ Use and update anti-virus software ▶ Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ul style="list-style-type: none"> ▶ Restrict access to cardholder data ▶ Assign a unique ID to each computer user ▶ Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ul style="list-style-type: none"> ▶ Track and monitor access to cardholder data ▶ Test system security regularly*
Maintain an Information Security Policy	<ul style="list-style-type: none"> ▶ Maintain business policy to address security

* Finally, and few people actually know it, but PCI DSS does mandate an annual formal risk assessment, not just a list of controls to implement! The Requirement is 12.1.2. Merchants need to check the requirements in their states.

While this is a simplified version of the requirements it comes down to a few simple and relatively inexpensive enhancements.

- ▶ Use a firewall and anti-virus software and keep it current.
- ▶ Set up individual user id's and passwords for everyone who has access to your computers. Do NOT use default passwords. Rule of thumb from a forensic technician: passwords should be at least 8 characters, at least 1 capital, 1 number and 1 symbol. It need not be "p6*y3smw?" if that means nothing to you. "4maDame%" (for madam X) is fine.
- ▶ Do not keep credit card numbers (or employee social security numbers or any other private information) stored with public information in a computer's data base. Before you say, "We keep those numbers in another field and no one knows it's there and it's not labeled," here's an interesting report: "About 600,000 [XX's] customers got a shock earlier this month when they received their annual tax documents with their **Social Security numbers** printed on the outside of the envelope. (dated February 24, 2010)" This could have been avoided if the social security numbers had been in a completely different restricted file. As it was, (note the past tense) during a routine mail merge a very costly mistake was made.
- ▶ Encrypt all transmissions of data and any private data stored on the computer system. Do not keep what you do not need.
- ▶ Write down and maintain your policy for safeguarding private information, what information is collected and stored, how it's used, stored and destroyed. Include who has access to the information and why. Write it down. This could help to save your business in a civil suit if it's written down and being followed as a part of routine business.
- ▶ Test your safeguards periodically. Don't ask employees if they are following established security procedures, observe them. When major software updates occur or hardware is replaced, do a check and make sure everything is still secure.

Why should you comply?

The answer is not to avoid fines although there will be fines. However the negative consequences are so much greater than just fines. Your store's contract with your bank probably has a clause in it that states that any fines from the card brand will be "passed through" to you, the merchant. If you are both noncompliant and compromised, higher fines may be imposed. At the discretion of the Card Brand, you may have your designation level raised from a level 4 to a level 3 or higher depending on the breach. Believe it or not, if compromised, this will be the least of your concerns. Civil cases from

someone looking for the "easy life" at the expense of another can be astronomical and happen every day. Don't take the chance and don't get caught in the trap. Secure your data environment today!

Notes: This article is summarized from the massive amount of information at:

https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

If you are interested in more information on what to do if you suffer a security breach, here is a lengthy and detailed manual assembled by VISA (click here:

http://usa.visa.com/download/merchants/cisp_what_to_do_if_compromised.pdf

WHAT IS THE CORRECT WAY TO CALCULATE MARKDOWN % ?

~~~~~

I was talking to a vendor's rep this month and from what he told me, there are a number of retailers who are not calculating their markdown percentage correctly! Everyone needs to know the correct method. It is to take the markdown dollars (the difference between the original retail and the selling price) and divide it by the selling price.

When you put something on sale in your store and put a sign out for your customers that it is 40% off - THAT IS NOT A 40% MARKDOWN!! For you, the retailer, it is actually a 66.67% markdown.

EXAMPLE: Using an original retail of \$100 for ease in calculations, a 40% off price for the customer would be a retail selling price of \$60. The markdown is \$40. Therefore, to calculate the markdown percent you take: \$40 divided by \$60 (the selling price) and get 66.67%, not 40%.

Using the same original retail of \$100 and 50% off for the customer, the selling price is now \$50 and the markdown dollars are also \$50. That means the markdown percent is 100.00%. That's quite a difference! I hope you have been calculating your markdown percentages correctly. If not, now you know and we will all be on the same page.

## QUOTE OF THE MONTH

~~~~~

"Be sure not to drive into the future using your rearview mirror as a guide."

author unknown

INTERNAL CONTROL MANUAL

~~~~~

### Studies have shown that almost half of all your store's shrinkage is due to employee dishonesty!

If you can reduce shrinkage by 1% that is an additional 1% of profit for you. As the owner it is your job to provide the procedures, checks and balances to keep your employees honest. Also, consider that in this tough economic climate, normally honest people may become desperate. Financial need is one of the main reasons given for attempting theft from an employer. Make sure you are doing all you can to help avoid temptation before it strikes.

As a former controller for a 5-store chain of family apparel stores and with my experience working with retailers around the country as a retail management consultant I have developed a manual to help you with this. It is our "Internal Control Manual" that covers all aspects of a retail store's operations. It is set up in an easy question and answer format where a Yes answer means things are OK and a NO answer means you may have a problem that needs further checking.

To get a copy for your store, for just \$95 shipped Priority Mail, visit our website at [www.the-retail-advisor.com](http://www.the-retail-advisor.com) and click on the "Internal Controls" icon.

Do not wait until you discover that a trusted employee has stolen \$70,000 from you (like a retailer I know had happen to him). Take steps now to make sure your merchandise and cash are as safe as you can make them. Do not delay! Take 5 minutes now to order your copy.

## OPEN-TO-BUY

~~~~~

Announcing a new lower pricing structure for our Open-To-Buy Service.

If you are tired of trying to decide how much of each type of merchandise to buy when at market, or if you are having trouble with cash flow, you owe it to yourself to try using an Open-To-Buy. We normally find that retailers who follow an Open-To-Buy enjoy increased Sales, higher Gross Margin and Profit and better Cash Flow.

Now, you can have a professionally generated Open-To-Buy, including a monthly review by someone with over 30 years retail experience for as little as \$230 a month (after a one-time set-up fee that includes help with setting Stock Turn Rate and Markdown percentage goals and the development of an annual Gross Margin Plan by classification).

We do not require any long-term commitments so you can cancel with just 30 days notice. Call us at 1-877-206-1299, visit us on the web at <http://www.the-retail-advisor.com/open-to-buy.html> or send an email to LC@the-retail-advisor.com to get more information, sign up and get started on your way to a more profitable store.

WHAT WE DO . . .

~~~~~

- o [Monthly Open-To-Buy Service](#)
- o Open-To-Buy Implementation on Your System (if available)
- o Merchandise Performance Evaluation
- o [Shrinkage Control](#)
- o Development of Incentive Plans
- o [Development of Job Descriptions](#)
- o Seminars On Retail Subjects
- o Financial Analysis
- o Financial Budgeting and Cash Flow Projections
- o Computer/POS System Evaluation, Selection, Usage
- o Policy and Procedure Development
- o [Lead Tele-SWAP Groups](#) (Share With A Peer)