

## Prioritized Approach to PCI Compliance Doesn't Go Nearly Far Enough

by David Taylor



After breaches of at least two major card processors, the card brands and the standards committee are on the defensive and have finally bowed (somewhat) to the complaints of the merchant community by introducing a risk-based "Prioritized Approach framework" as a response to the recent data breaches of supposedly PCI compliant companies. Unfortunately, it does not go nearly far enough

The Prioritized Approach is basically a spreadsheet that uses numbers from 1-6 to roughly approximate the sense of risk that would be reduced by implementing each specific PCI requirement. This is the sort of tool that many security and compliance managers have been using for several years to prioritize their PCI projects. However, the spreadsheet is generic for all business types. There's no sense of customization of "risk weighting" based on the characteristics of a business (i.e., card acceptance channels) or IT infrastructure (i.e., network and data management). Please visit [www.pcisecuritystandards.org/education/prioritized.shtml](http://www.pcisecuritystandards.org/education/prioritized.shtml) to download this spreadsheet.

### Milestones Are Better Than Going 1 to 12

The best aspect of the Prioritized Approach is that makes it clear that merchants should not begin their PCI compliance efforts with requirement 1 and work their way through to 12, assuming that any organization actually manages PCI that way. The other useful aspect is that the tool provides the ability of merchants to visually show progress. Adding some risk focus shows that the card brands and the SSC are definitely moving in the right direction. But note that there is no guarantee that any acquiring bank or the card brands themselves will actually "honor" the submission of this tool as a show of progress and actually

delay the imposition of fines. Remember, the PCI SSC has nothing to do with the enforcement of compliance, which is done by the card brands and acquirers.

### The Standards Have Not Changed

In case anyone should read this and think the PCI standards have suddenly become "risk based" because they mentioned risk when they announced the tool, such is not the case. The 1.2 version of the standards is not scheduled to be updated until the fall of 2010.

Although I agree with the order and manageability that such a schedule provides, it does make it more difficult to adjust such an explicitly detailed standard to emerging threats and technologies that can change the "effective risk" associated with specific controls. Obvious examples that need to be addressed include the impact of tokenization on PCI scope, the impact of server virtualization on data access controls, and the impact of SaaS on data ownership and management.



### The Bottom Line

Every organization that collects, processes or stores credit or debit card data still has to comply with all 12 of the PCI DSS. The PCI SSC makes that very clear. The Prioritized Approach does not change the standards. It is a useful tool to help "beginners" understand security risks and help them proceed with the implementation of PCI compliance in a way that addresses the largest risks first. I see this primarily as "first pass" at adding risk awareness, as well as an interesting artifact of the industry's scramble to address merchant complaints and avoid increased regulation or even "nationalization" of the payment card industry along with the banking industry.

## 7 Steps for Increased Retail Sales



**Step 1:** Always know your business inside and out. Make it your business to know stock status, available delivery times and advertising schedules and promotions.

**Step 2:** Create an atmosphere that your store is having the biggest sale of the year. Make sure that your store reflects the event. Look busy and successful.

**Step 3:** Remain upbeat and be in a positive state of mind. "This is the place to buy your product" should be written all over your face.

**Step 4:** Know your competition and all of their strengths and weaknesses. Know your industry and all of the corresponding product information.

**Step 5:** Fully embrace your product and what it can do to make life better for your customer. Having confidence in your product line and the place that you work will allow you to make many more and higher end sales.

**Step 6:** Always be prepared with the proper sales ads, price sheets, costs and product information at hand. Looking and acting organized makes a difference to the customer.

**Step 7:** Always use proper and friendly body language. How you look, stand and act are windows to the soul. Make sure you let your customers know that you are not hiding anything or lying to them.



Prioritized Approach to PCI Compliance Page 1



7 Steps for Increased Retail Sales Page 1



Product Spotlights Page 2



The Retail Legal Advisor

Page 3

## Receive **10% Off** of your Software Assurance or Support Contract

Make sure that you have the latest updates and technical support to run your systems smoothly. Renew by **3/31/2009** and receive **10%** off of your Software Assurance or Support Contract. Don't let this **limited time** opportunity pass you by! **Contact Marisol** at 800-513-5917 ext.132 or by email at MarisolC@RetailTechnologyExperts.com to take advantage of this special offer.



## Improved Invoicing Process

In order to ensure efficiency in our processes as well as to keep costs low for our customers, Retail Technology Experts will **no longer be sending out paper statements or invoices**. These will be now be delivered via email. Please **contact Arly** to provide your email address in order to ensure proper delivery

### Contact Arly

Phone: 800.513.5917 ext. 111

Email: ArlyA@RetailTechnologyExperts.com

## Meet the Staff at Retail Technology Experts

### Karen Dillen

Retail Systems Consultant



Karen Dillen joined the team at Retail Technology Experts in November of 2008 and is part of our San Diego, CA office. She brings with her over 10 years of retail experience in various industries as well as POS sales experience. As a

Retail Systems Consultant, Karen enjoys building relationships with customers and prospects. She takes pride in making a difficult decision, like choosing the correct point of sale solution, as simple and painless as possible for our customers.

Karen holds a BS in International Management from Georgetown University. Karen spends her spare time watching her sons' lacrosse and baseball games. She also enjoys skiing, photography, and traveling.

### Contact Karen

Phone: 1-800-513-5917 ext. 404

Email: KarenD@RetailTechnologyExperts.com



## Product Spotlight

### Creating Purchase Orders and Printing Tags

#### Creating Purchase Orders

Path: Purchasing, Purchase Orders, New

- Enter vendor code (use lookup button to create new vendor, save vendor, click to assign to new PO).
- Enter order, ship and cancel dates if applicable.
- Choose/Edit Items form on top, then "new" on the top left. Enter item information (DCS, style, description, DOC QTY, DOC Cost, original price), then save, click new to enter next item. Leave blank any field that is not applicable to the new item.
- If you use Copy-New-Paste, remember to uncheck the window to "break the style" and change any entries that differ from the "copied" item. Once you are done entering all the new items, click ok on side menu to go back to PO.
- Save on top left (optionally enter instructions if needed). Print PO by clicking print on top.

#### Receiving and Printing Tags

Path: Purchasing, Vouchers, New

- Enter PO being received (use look up button to see list of purchase orders). Select PO items on side menu to see items on PO.
- If everything due is being received, click receive due, then click Ok on side menu. If doing a partial receiver, use DOC QTY column to enter partial quantities being received, click ok when done.
- Back on Receiving Voucher, enter freight and fees if applicable; spread cost only if accounting confirms this. Use Comments fields to track comments about the receiver.
- Print tags on side menu, select "All Listed Records" so all items on voucher gift tags printed.
- Update only or print/update on side menu if you want a printed copy of the receiving voucher.



## Product Spotlight

### Defining Specific Customer Data Fields

Did you know when capturing your customers' information in Microsoft RMS there is the ability to define specific fields of data you would like to collect?

- There is a tab available under each record called 'Additional'.

This area allows you to define up to 5 text field, 5 date fields, and 5 numeric fields.

- Once these fields have been defined, the information can be used to:

1. Display on the HTML portion of your POS screen. These fields can be selected and shown as a quick reference to the cashier. This will assist them in knowing a bit more about the customer's account.

An example would be showing 'Favorite Brand' so you can recommend certain items or upcoming specials.

2. Utilize the advanced 'Find' option on the Customer lookup screen to search for information in these fields.

An example would be searching for all customers with 'Size' 10. If needed, click Find to display the Find Items window.

3. Run the 'Customer List' report and add the defined fields as filtering options or columns to display on the report.

An example would be showing all customers with a 'Birthday' in May. This will assist in emailing/mailling them a special discount.

- To define these fields access Store Operations Manager.

- On the File menu, click Configuration, click Captions, and then click the Customer tab.

## The Retail Legal Advisor



by: Michael Berger, Esq.

### Expansion of the Americans with Disabilities Act ("ADA")

In 2008, Congress passed the Americans with Disabilities Amendments Act of 2008 ("ADAAA"), which expands the scope of the ADA (passed in 1990). The ADAAA took effect on January 1, 2009.

Under the ADA and the ADAAA, a disability is defined as a "physical or mental impairment" that "substantially limits" a "major lifetime activity" (key terms are quoted). Many courts have interpreted the quoted phrases and have limited the scope of the ADA by narrowly defining "major lifetime activity" and "substantially limits".

Congress, in passing the ADAAA, has attempted to broaden the scope of these terms in several ways. For example, the ADAAA provides that the Equal Employment Opportunity Commission's ("EEOC") current definition of "substantially limits" as "significantly restricted" is too high a threshold and orders the EEOC to redefine the term to a lower level of limitation. The ADAAA also specifically states that employers and courts may no longer consider mitigating measures (e.g. medicine, hearing aids etc.) in deciding whether an impairment reaches the level of a disability.

Regulations and interpretations associated with the ADAAA are currently in a state of flux. As a result, any employee requests for accommodation or issues involving an employee's ability to perform his or her job because of an impairment, should be directed to the employer's human resources department and/or its attorney for review and guidance.

#### Contact Michael Berger

Michael Berger, Esq.  
 Carpenter & Berger, PL  
 954-772-0127  
 mberger@carpenterberger.com  
 www.carpenterberger.com

Disclaimer: The information provided in the Retail Legal Advisor column should not be considered legal advice. This column is intended only to provide general educational information. You must never rely on the information provided here as legal advice. Only your attorney can evaluate your specific situation and provide you with legal advice. Except as provided below, you may feel free to forward, distribute and copy the Retail Legal Advisor column, as long as you forward, distribute and copy it without any changes and include all headers and other identifying information. You may not copy it to a website without the author's prior written consent.

## Customer Success Story Nest Casa



Nest Casa is a luxury furniture and home accessories brand focused on offering unique, high quality European products. Based in Miami, Florida, Nest Casa has one retail location in Miami Beach as well as a warehouse facility nearby. Both locations are currently running Retail Pro software on HP RP5700 retail hardware systems.

With a separate warehouse location to manage in conjunction to their retail location, Nest Casa needed help finding the best way to have one system control their inventory and point of sale needs. By implementing an integrated Quickbooks Accounting link, Nest Casa is also able to directly share information with its accounting system. "During our initial meeting, Retail Technology Experts sat down with us and helped us figure out what we needed. They showed us Retail Pro and helped us identify what aspects of the software would work best for what we were trying to do," said Sara Colombo, President of Nest Casa.



As a first experience with point of sale software, Nest Casa needed plenty of help learning about Retail Pro. "Alex handled our installation and training. He was a great teacher, very patient, and made sure that we understood everything. He also helped customize our systems to make sure that we were getting the most out of them," said Colombo.

The best part of working with Retail Technology Experts was their expertise. "The team at Retail Technology Experts was always very knowledgeable. They were honest about selling us only what we were really going to use and they let us know what would be cost-effective and what wouldn't be," mentioned Colombo.

Nest Casa plans to continue expanding in the future, moving into E-Commerce as well as opening additional retail locations.

#### RETAIL OPTIMIZER

Editor/Design: Laura Gonzalez  
 800.513.5917 ext.124  
 LauraG@RetailTechnologyExperts.com