Sage Payment Solutions

# **Reduce Your PCI Liability** with Integrated Payment Solutions

Emerging Payment Card Industry (PCI) standards have turned up the heat on companies that deliver solutions involving payment processing. In July of 2010, the Payment Application Data Security Standard (PA-DSS) mandated that all applications, whether installed or web-based, be compliant or face stiff penalties associated with non-compliance. The costs in time and resources to ensure you keep your company and clients protected from fraud can be extremely high. Additionally, breaches and heavy fines for non-compliance continue to rise along with the hassles of working with multiple service providers. As hard as you try, you may not even be sure you're fully compliant due to the gray areas involved in understanding and adhering to the standards.

In this paper, you'll learn about the top risk areas associated with PCI standards and how an integrated payment solution can help minimize those risks.

"I know payments security is important, but I don't think I knew what measures needed to be in place to be compliant at the outset."

**Jessica Granda**
Treasurer, Grandall Distributing Co., Inc.
(Sage Peachtree customer)

## About PCI and PA-DSS

The PCI Data Security Standard (PCI-DSS) is designed to ensure that ALL companies that collect, process, store or transmit protected credit card information maintain a secure environment for these purposes. Standards and requirements are managed by the PCI Security Standards Council, which is an independent body created by major payment card brands like Visa®, MasterCard®, American Express®,Discover® Card and JCB®. Although the PCI council maintains the standard, the payment card brands and acquirers are responsible for enforcing compliance.

The Payment Application Data Security Standard, or PA-DSS is a standard also managed by the PCI council. PA-DSS, which aims to prevent developed payment applications for third parties from storing prohibited secure data, provides a definitive standard for software vendors. Companies like yours that develop applications involving payment processing cannot collect, process, store or transmit prohibited secure data including magnetic stripe, CVV2 (card verification value), PINs (personally identifiable numbers) or PANs (primary account numbers). The standard also stipulates that you ensure your applications are PCI compliant.

## What You and Your Customers Might not Know about PCI Compliance

While most business owners know that security is important, ensuring compliance with PCI security standards can be challenging. Keeping up with evolving regulatory requirements and fees for different types of payments is another headache.

**A recent survey conducted by the SMB Group found there's still a significant percentage of small to medium-size business owners who aren't familiar with PA-DSS requirements and fees.**

- 45 percent who don't currently use integrated payment solutions either haven't heard of PA-DSS or don't know how it applies to their business
- Only a third that use integrated payment solutions understand the fees and risks of non-compliance, leaving the other two-thirds unaware of requirements and risks

## The most common myths about PCI compliance include:

1. *My customers don't have enough volume of business to have to worry about compliance.*

There are four volume-based merchant levels defined by Visa. Level 1 merchants process more than six million Visa transactions per year and, therefore, must meet specific requirements. Transaction volume goes down as the level numbers increase, with Level 4 merchants processing fewer than 20,000 e-commerce transactions or up to one million of any type of transaction. Essentially, any business who accepts card payment in-person, over the phone or online must maintain compliance.

2. *I have an SSL certificate and therefore I'm compliant.*

High assurance SSL (Secure Sockets Layer) certificates provide only the first level of customer security. Since July 2010 all merchants who process via the internet must also ensure that there is a secure connection between the customer's browser and the web server. Merchants must also validate the payment processors' website operators are legitimate, and that the processors are meeting the PCI requirements also. In addition to the above requirements, a quarterly scan by a PCI SSC (Security Standards Council) approved scanning vendor is required.

3. *My customers are mostly small or medium-sized businesses and data security breaches mostly happen to large companies.*

Small to medium-sized companies are breached every day. We just don't hear about it because their names aren't well-known enough for the stories to be reported by popular news outlets. According to the 2011 Trustwave® Global Security Report, greater than 80 percent of all payment data breaches are with small business merchants, either directly through their in-house infrastructure or through their third-party solutions. In the same report, Trustwave cited that 88 percent of breaches last year were caused by the way in which software integrators implemented a software solution for a merchant. As awareness (and pain experienced first-hand with breaches) rises amongst small and medium-sized business owners, it will be nearly impossible for a software vendor wanting to provide a payment processing solution to stay in business without becoming PCI compliant.

4. *I use a third-party payment processor so I don't have to worry about compliance.*

Using a third-party company for payment processing can help reduce risk, but doesn't mean the business can ignore PCI requirements. **For example, it's common for a business to have multiple merchant IDs for different terminals or cash registers. If the merchant IDs are from different industries and different locations, then the merchant IDs can be** "chained" if they have the same Tax ID and the Self Assessment Questionnaire is completed for the most risky of industries and processing methods. The only time several Tax IDs can be "chained" is if they are using the same stand-alone dial out terminal and have the same location. Third-party solution providers who only "pass through" credit card information without storing it aren't exempt from the burden of compliance either. According to the standards, if the software provides a user interface for customers or merchants to enter their credit card information and that information is then transmitted to a processor, the software provider already meets two of the four criteria that put them in scope for the need to be PCI compliant.

Many small and medium-sized companies do not have the resources to fight the fines, lawsuits and loss of business due to negative public perception once there is a security breach.

## The Price of Non-Compliance is High

Many business owners put off taking action because of the costs involved in putting security measures in place and getting regular assessments. What they may not understand is the cost of non-compliance could be much higher. For example, major card companies—at their discretion—can fine acquiring banks between $5,000 and $100,000 per month for compliance violations. Banks will most likely pass those fines along, affecting merchants.

Several high-profile security breaches have been reported already in 2011. In June, banking giant Citigroup® announced it discovered a security breach in which a hacker accessed personal information from hundreds of thousands of accounts. This bad news helped accelerate the downward spiral as their stock plunged 15 percent in just a month. In April, Sony® announced that credit card data of its PlayStation® users "may have been stolen" in an intrusion that caused its PlayStation network to be down for a week. Analysts estimated that the incident could cost Sony more than $1.5 billion in card replacement costs alone.

Although they owe millions in fines and will pay more in protracted legal actions, big corporations have the resources to overcome these damaging setbacks. Small and medium-sized companies do not; many wouldn't survive the fines, lawsuits and loss of business due to fear of continued

**To assure shoppers and stay competitive, your customers need to maintain compliance. They're relying on you to provide hassle-free products and services.**

Your customers need to maintain compliance to meet demand. Their customers want to do business with companies they trust who offer the convenience of paying with credit or debit cards in-person, over the phone, and online. Your customers rely on you to provide hassle-free products and services. You, in turn, would benefit from working with just one payment solution provider versus several to meet your customers' secure payment processing needs.

exposure and negative public perception. And while their third-party software providers may not be subject to the host of costs and fines passed down from major credit card companies to merchants, the likelihood of the merchant filing a lawsuit to recoup the costs associated with a breach is extremely high.

## Reduce PCI Risk with an Integrated Payment Solution

For all practical purposes, it's simply not possible for you to continue to grow your business without becoming PCI compliant. The risks of non-compliance or having to recover from lawsuits and negative publicity caused by customers' breaches are too high. If you're tired of investing precious resources trying to maintain requirements and working with multiple vendors to provide payment-related services to your customers, it's time you consider an integrated payment solution.

An integrated payment solution, such as Sage Payment Solutions with the Sage Exchange Payments Hub, can help you streamline operations with a single vendor/point of contact solution. **Sage Payment Solutions provides a "PCI-free zone" which allows you to add payment processing to your product offering without adding the compliance burden to your company. And, Sage Payment Solutions is the only vendor that enables integration of your applications to other Sage solutions.**

**When you're ready to save time, reduce risk and deliver greater value, contact Sage Payment Solutions at 800-852-1903 or www.sagepayments.com.**

**Sage Payment Solutions**
1750 Old Meadow Rd, Suite 300
McLean, VA 22102

Phone: 703-848-2980
Toll Free: 800-261-0240
Fax: 703-848-9457

www.SagePayments.com