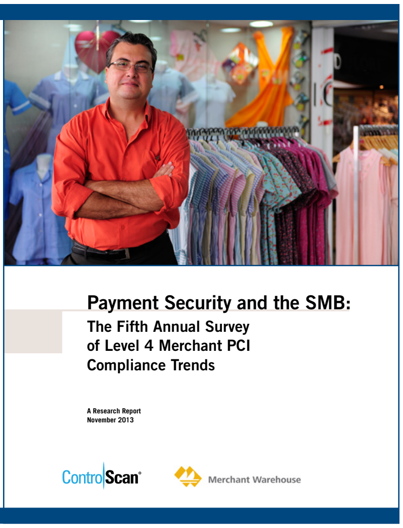
Level 4 Merchant PCI Compliance: Five Best Practices

ControlScan®



Payment Security and the SMB:
The Fifth Annual Survey of Level 4 Merchant PCI Compliance Trends

A Research Report
November 2013

ControlScan
Merchant Warehouse

Does your business fit into MasterCard's Level 4 merchant group? If it does, you're not alone. Representing 98% of all U.S. retailers and primarily comprised of small to mid-sized businesses (SMBs), merchants in the Level 4 group number in the millions.

While they are certainly part of a diverse group, Level 4 merchants share important characteristics when it comes to securing the data they capture during the electronic (e.g., credit/debit) payment process. These commonalities can make Level 4 merchants an attractive target for data thieves.

The Level 4 Merchant Security Landscape

Since 2009, ControlScan has conducted an annual survey to better measure and understand Level 4 merchants' challenges in understanding payment security best practices and complying with the Payment Card Industry Data Security Standard (PCI DSS). Our most recent survey was conducted in late 2013, in partnership with Merchant Warehouse.

Awareness is Up, But Response Comes Up Short
A solid majority (69%) of this year's survey respondents say they are at least "somewhat familiar" with the PCI DSS. And year-over-year data indicates that as a group, those merchants *who are aware* are making progress:

- The percentage of merchants validating compliance grew substantially, from 50% in 2012 to 70% in 2013;
- At 40%, the number of merchants who agree that complying with the PCI DSS makes them "much more secure" is significantly higher than those who disagree (28%); and
- There has been a significant increase in merchants' understanding of why the PCI DSS applies to their business.

The above statistics are certainly encouraging, but there is more work to be done when it comes to Level 4 merchants' response to the payment security threats that plague their space:

- The vast majority continue to think they are at little-to-no risk for data compromise;
- Should a breach occur, 64% have no formal incident response plan in place and are therefore unprepared to quickly and properly address the situation; and
- More than one-third of those who are aware of the PCI DSS did nothing PCI related in the last year, with the exception of "completing the paperwork."

Where to Go From Here: Five Best Practices

The best way to truly strengthen your business's security posture—which is the goal of the PCI DSS—is to have a sober understanding of your risk as well as the full scope of your PCI compliance responsibility. To that end, ControlScan has assembled the following best practices for easily and cost-effectively protecting your business against data thieves.

1. Understand Your Sensitive Data, Where It Is, and Who is Responsible for its Protection.

Owners of even the smallest businesses need to understand what happens to each customer's sensitive data as soon as it leaves the customer's hands and enters the business's data processing, storage and transmission systems. As the customer's information moves through your business processes, it is critical to maintain that data's security and integrity.

Sensitive data can be financial information, such as credit card numbers, as well as any personally identifiable information (PII) that can be linked to an individual. Be sure to understand and identify all the places within your office environment, business processes and systems that sensitive data is captured, exchanged or stored.

Responses to the 2013 Survey of Level 4 Merchant PCI Compliance Trends show that formal responsibility for information security typically falls on the person who heads the organization or no one at all. A significant first step to putting security controls in place is assigning individual responsibility and accountability for monitoring and protecting the sensitive data your business handles. We suggest creating a simple spreadsheet that documents the various types of sensitive data your business is handling, its location, and who has responsibility for it. Be sure to review this spreadsheet on a quarterly basis at minimum, to ensure that the information it contains remains current.

2. Avoid Storing Sensitive Data—And If You Have To, Secure It.

One of the easiest steps toward lowering the security risk to your business (and reducing your scope for complying with the PCI DSS) is to not store cardholder data, period. Examine the spreadsheet you created as part of Best Practice #1 to evaluate where your sensitive data resides. Ask yourself with each line item: *Does this information really need to be retained and stored?*

The more items you can remove from your spreadsheet (because you aren't storing the data), the better. If there is a significant business reason for you to store sensitive data, the following steps will help you secure it:

- Limit database access to only those who absolutely need it, giving those parties their own, unique credentials;
- Do not store authentication data for either your employees or your customers; and
- Implement a tokenization solution to enable repeat online customers to securely store and access their payment information.

Again, the best thing you can do for your business is not store cardholder data or PII at all.

3. Protect Your Perimeter with Firewalls; Ensure You Don't Leave Back Doors Open.

Good security incorporates "defense in depth," or multiple layers of protection. One of the primary requirements of the PCI DSS is to have a properly configured firewall in place, because for businesses with an Internet connection, firewalls are a first line of cyber-defense.

It is imperative to properly configure your firewall according to the way your business handles data. The issue with "plugging in and forgetting" your business's firewall is that a poorly configured firewall is only slightly better than no firewall at all. According to the United States Computer Emergency Readiness Team (US-CERT), the most common configuration mistake is not providing outbound data rules, which can permit communication to untrusted systems and potentially lead to data compromise.

Protecting your perimeter means checking for any unprotected holes that could allow attackers to gain entry. The most common mistake is a remote access service that remains in a constantly enabled and running state with a weak, or even worse, a default user-id and password in place. This often happens when consultants, contractors or VARs want to conveniently access business systems remotely in order to provide support. You can mitigate this security risk by limiting remote access to your network, ensuring remote access is only enabled when it has to be, and requiring vendors to use two-factor authentication for access.

If your business utilizes Internet-facing Web applications—in particular, an ecommerce site that accepts card payments—requirement 6.6 of the PCI DSS requires that you either utilize a Web Application Firewall (WAF) or have your website reviewed annually (or after any changes). Most merchants don't have the resources to engage a technical expert to review their site after changes, so a WAF is the optimal alternative.

4. Fortify Your Interior with People, Procedures and Technology.

One of the weakest links in the security chain is humans—your employees; therefore, security awareness training is a critical, ongoing requirement for all employees, no matter the size of the business. Level 4 merchants should conduct security awareness training on an annual basis and include specific instructions for how employees should handle sensitive information and credit card transactions.

The following are additional tips for enacting this best practice:

- Vigilance is required on the part of all employees, but especially on the part of the person you've made responsible for monitoring and protecting your business's sensitive data;
- A comprehensive security policy is essential and should include a checklist to ensure important security points are reviewed on a regular basis; and
- Like the security policy, an incident response plan is a proactive way to shield your organization against worst-case scenarios.

From a technology standpoint, merchants must be using payment technologies that have been tested, validated and listed by the PCI SSC; including but not limited to PA-DSS validated applications and PTS validated devices.

In addition to segmenting the card data environment away from the rest of the network, it's important to keep commercial grade anti-virus protection actively running and current on every machine. Follow your technology vendor's recommendations for installing and using every patch and service kit released for your systems and applications.

5. Know Your Service Provider(s) and *Their* State of PCI DSS Compliance.

Today, many small merchants are outsourcing all or part of their card processing steps to service providers, such as shared hosting providers, payment gateways, managed security firms, etc. It is typical for merchants to outsource all or part of their IT infrastructure to service providers as well. Unfortunately, more than half (51%) of respondents to the 2013 Survey of Level 4 Merchant PCI Compliance Trends said they do not require their third-party service providers to be PCI compliant.

A service provider's inability to properly protect your customer data could implicate your business should a breach occur. Protect yourself by asking for proof of compliance, as well as requesting any other audit reports such as the SAS 70, or its successor, the SSAE 16. These reports are often held by larger companies that store and/or process financial or other critical information on behalf of others.

MasterCard maintains a list of PCI DSS-compliant service providers. The following are tips for evaluating, establishing and maintaining relationships with your outsourced service providers:

- Create a due diligence list for choosing new service providers. Your list may include items such as the provider's disaster recovery/business continuation plans, the number of PCI clients the provider serves, whether the provider maintains policies and procedures for the services they offer, how long they've been in business, etc.
- Keep a list of your current service providers; include their PCI DSS compliance status. (Check up on their status at least annually.)
- Have a written agreement with your service providers; make sure service providers acknowledge their responsibility for the security of the cardholder data they touch.

For most Level 4 merchants, technology and data security are foreign and frustrating concepts. If you're in a place where you would rather run your business than worry about hackers and security threats, PCI DSS-compliant service providers are the way to go.

Security is Everybody's Business

Just as you rely on the merchants you shop with, your customers are depending upon you to protect their sensitive information. As a small business owner, it is your responsibility to take threats to your business systems seriously so that consumer information can be protected. Your customers won't thank you, because they will never know how you've protected them behind the scenes. But the alternative (fines, penalties and lost business) is not worth the risk.

Click here to download the entire ControlScan white paper, *The 5 Data Security Best Practices for Small Merchants.*