A Tale of Two Merchants:

The Fourth Annual Survey of Level 4 Merchant PCI Compliance Trends

A Research Report
November 2012

Table of Contents:

EXECUTIVE SUMMARY:

Security awareness and activity gaps persist between brick-and-mortar and ecommerce merchants.

Since 2009, the Payment Card Industry (PCI) compliance and security experts at ControlScan have undertaken an annual survey measuring Level 4 merchants' engagement with the PCI Data Security Standard (DSS). The previously reported results have informed payments industry professionals of the data security and risk-related issues they should proactively address within this important segment of the U.S. marketplace.

This year's survey, conducted in partnership with Merchant Warehouse, a leading innovator of payment and program acceptance solutions, represents a significant contribution to the overall objective of this study set in that trends are revealed by examining the year-over-year results. With four years of data now in place, we can begin to discover areas where Level 4 merchants have shown improvement as well as areas requiring greater action from the ISOs and acquirers serving them.

What we now know is that ecommerce merchants are continually outpacing brick-and-mortar (B&M) retailers in their awareness and action related to PCI compliance and overall data security. Compared to their ecommerce counterparts, B&M merchants are significantly less likely to have completed the PCI compliance process, as they are less aware of the PCI DSS and the possibility that their customers' sensitive information could fall into the wrong hands. Perhaps because of the card-not-present (CNP) aspect of Internet transactions, ecommerce merchants appear to be more cognizant of the action steps required for securing customer data.

This research report discusses the concerns raised following four years of complacency demonstrated by Level 4 merchants in general, as well as the security risks Level 4 B&M merchants face if the awareness-and-action gap persists between them and their ecommerce counterparts. We will review the 2012 survey's methodology, audience profile and key findings, and then move into a detailed, question-by-question analysis followed by our recommended action steps for ISOs and acquirers.

Level 4 merchants, as defined by Visa, are merchants processing less than 20,000 Visa ecommerce transactions annually. For brick-and-mortar and other retailers, Level 4 merchants are those that process up to 1 million Visa transactions annually.

Data breaches: The big picture for small business

The objective of the PCI DSS Compliance Survey is to provide insights and recommendations that help ISOs and acquirers better serve their merchants while reducing their own risk exposure. Much has been published about the consequences of PCI non-compliance, as well as small merchants' connection with data compromise. It's important that ISOs and acquirers monitor this information for its value in educating those within their merchant portfolios.

Here is a summary of recent data breach statistics as observed by financial and payments industry experts:

- **Small businesses are being specifically targeted by hackers.** A June 2012 Visa presentation confirms that attacks against Level 4 and franchise merchants are on the rise in the United States. These merchants are an ideal target for automated attacks from cyberspace, because they often fail to implement basic data security best practices. In its presentation, Visa notes a 15% increase in the total number of reported compromise events from 2010 to 2011 alone, and from 2009 to 2011, 70% of compromise events involved B&M merchants.

- **There is a correlation between PCI non-compliance and data breaches.** According to the Verizon 2012 Data Breach Investigations Report, 96% of last year's breach victims were not PCI compliant. Indeed, many industry experts believe that PCI compliance validation provides a telltale sign that the compliant business is concerned and proactive about data security.

- **No one expects a data breach, but breaches do happen—and the resulting losses are often catastrophic.** Symantec's 2011 Cost of Data Breach Study found that merchants' direct costs of recovering from a security breach average $194 per stolen record. And in their 2012 National Small Business Study, Symantec and the National Cyber Security Alliance discovered that 47% of small business owners think a data breach event at their business would "have no impact."

- **Preventive measures are generally quick and inexpensive to implement.** In 63% of last year's data breach incidents, preventive measures would have been "simple and cheap," according to Verizon's 2012 Data Breach Investigations Report. Best practices for preventing a data breach include changing default user-id and password combinations on POS systems and then restricting access to that information. In addition, Verizon recommends (and the PCI DSS requires) a properly-configured firewall to provide a first line of defense against external attacks. A top 5 list of small merchant data security best practices, produced by ControlScan, can be found here.

- **Security is just plain good for business.** Edelman, a national PR firm, polled more than 4,000 consumers for its 2012 Privacy and Security Study. Eighty-four percent of the study's respondents said information privacy and security are very important to them when purchasing products online; however, only 33% said they trust online retailers to properly protect their personal information. Security concerns extend to brick-and-mortar locations, too. For example, many restaurant patrons worry about card-skimming activities and prefer to pay at a terminal instead of giving their payment cards to servers for processing.

METHODOLOGY AND AUDIENCE PROFILE:

Conducted in August 2012, this year's survey was sent to randomly selected Level 4 merchants listed in the databases of two separate entities:

- ControlScan, an expert provider of PCI compliance and security solutions designed for small merchants and the acquirers who serve them, and
- Merchant Warehouse, one of the largest independent sales organizations (ISOs) in the credit card processing industry.

The survey was completed online by a total of 603 merchants. The population of responders had the following characteristics:

Audience profile by...	Percent of responses
Merchant type:	
Retail/brick-and-mortar	44%
Ecommerce	16%
Mail/telephone order, hybrids, and other	40%
Respondent's title/function:	
CEO, President, Owner	70%
Finance	18%
IT	4%
Manager or Supervisor	6%
Other	2%
Number of employees:	
1 to 10	80%
11 to 50	15%
51 or more	5%
Annual transaction volume:	
Under $100,000	48%
$101,000 to $250,000	32%
$251,000 to $500,000	15%
$501,000 to $1,000,000	5%

KEY FINDINGS:

1. Level 4 merchants are missing the point of the PCI DSS.

Four years' worth of data reveals that as a whole, small merchants are unaware of their vulnerability to data breaches. In fact, PCI-related awareness and attitudes are in a holding pattern for Level 4 merchants, large and small, ecommerce and brick-and-mortar alike. Clearly, merchants—especially micro-merchants (those with 10 or less employees)—don't have PCI compliance and data security on their radar as a critical, ongoing business process that contributes to their overall success.

The 2012 survey validates two trouble spots that have been highlighted in ControlScan's past surveys:

- Forty-seven percent of respondents are "unsure" or "not at all" familiar with the PCI DSS, and
- Seventy-nine percent of respondents think there is little to no chance a data breach will happen to them.

The above findings represent a stubborn year-over-year trend of minimal growth in awareness and overall indifference in perceived risk. For B&M merchants, the trend is even more disturbing, because their levels of awareness and concern fall well below those of the ecommerce merchant respondents.

The overall lack of small merchant growth in terms of PCI compliance and data breach awareness should sound the alarm for ISOs and acquirers, prompting their swift response. While the recent ControlScan Acquirer Study found that the majority of ISOs and acquirers have a PCI compliance program in place for their Level 4 merchants, it's evident that merchants are not getting the message about the PCI DSS and its value to their business. Additional steps must be taken now to implement the clear, consistent and value driven communications that will successfully trigger merchant awareness and action.

2. Merchants familiar with PCI often contradict their own security-related claims.

On the surface, those merchants who are familiar with the PCI DSS appear to be very supportive of measures to protect sensitive data. Three positive signals emerged from the 2012 study:

- Overall, 77% of respondents say security ranks "medium" or "high" in terms of their organization's overall priorities,
- Sixty-seven percent believe that complying with the PCI DSS makes their business more secure, and
- When asked if they think the PCI standard should apply to their business, 57% of respondents say "yes."

Answers to other survey questions, however, erode the initial optimism:

- Of those respondents who have validated PCI compliance, only 39% claim that they have the documentation to support their Self-Assessment Questionnaire (SAQ) responses. Brick-and-mortar merchants are only half as likely as their ecommerce counterparts to have this documentation.
- Forty-three percent of respondents say they took no action nor made any purchases to achieve their PCI compliance—they "just completed the paperwork." The conspicuous absence of compliance-related activities (other than paperwork completion) suggests that many small merchants may be taking a check-the-box approach to data security.
- Only 50% of those aware of the PCI DSS have completed the compliance validation process. Ecommerce merchant respondents are above the average at a 70% completion rate, while B&M merchants are below the average at 45%. When all 603 survey respondents are included in the calculation, the overall PCI compliance rate for these Level 4 merchants drops to 30%.

In view of the entrepreneurial orientation of most Level 4 merchants, their confusion or disinterest on data security issues is hardly surprising. Merchants' need for security-related education and support further underscores the opportunity ISOs and acquirers have to proactively serve as a trusted advisor and business enabler, thereby demonstrating the value of the PCI program they are providing.

3. Ecommerce and larger Level 4 merchants are compliance leaders among their peers.

According to estimates by Visa, in June 2012, there were a total of 7,619 U.S. merchants in Levels 1, 2 and 3, and about 5 million Level 4 merchants. At that time, Visa reported the following rates of PCI DSS compliance validation, noting that "Level 4 compliance is moderate among stand-alone terminal merchants, but lower among merchants using integrated payment applications":

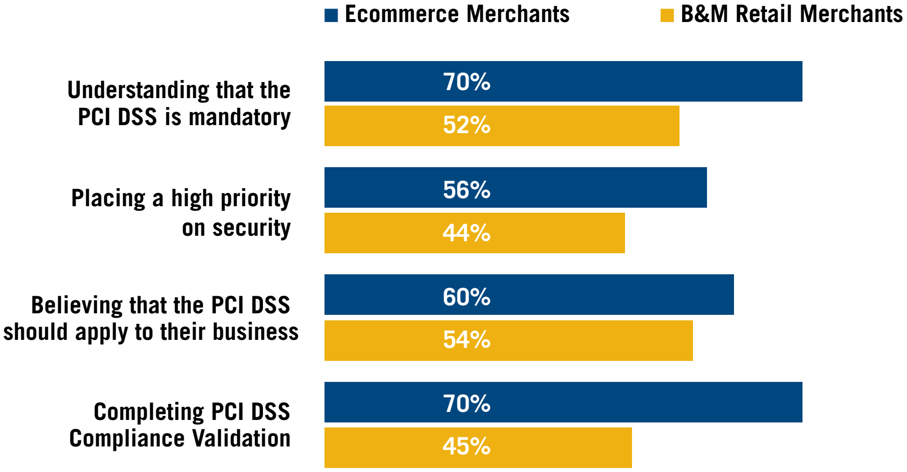
Level 1 merchants	**97%**
Level 2 merchants	**93%**
Level 3 merchants (ecommerce only)	**60%**
Level 4 merchants	**Moderate**

Data source:
http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf

Level 4 merchant compliance is not easily measured, but the last four years' data from the annual ControlScan/Merchant Warehouse Level 4 Merchant Survey show an important distinction between merchant types within this category. Namely, ecommerce merchants and larger Level 4 merchants (i.e., those with 51 or more employees) are setting the example.

In addition to the areas discussed in Key Findings 1 and 2, ecommerce merchants also lead in the following:

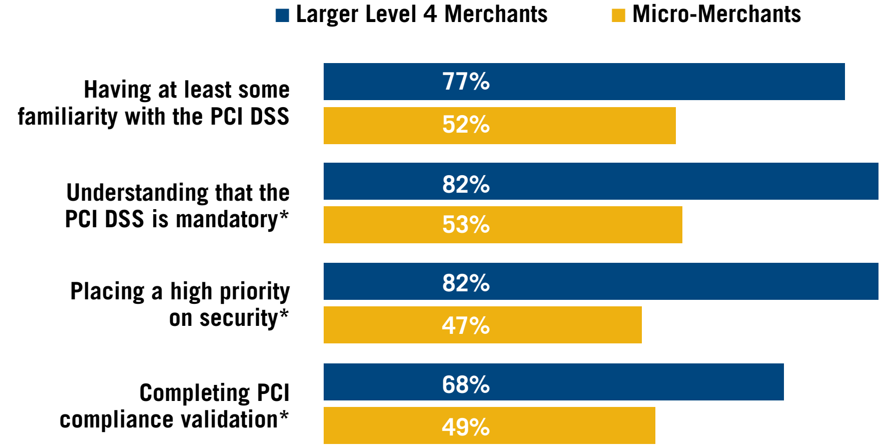
The Ecommerce vs. Brick-and-Mortar PCI Gap*



*Represents respondents who are aware of the PCI DSS

Level 4 merchants with 51 or more employees also lead micro-merchants in the following:

The Larger Level 4 vs. Micro-Merchant PCI Gap

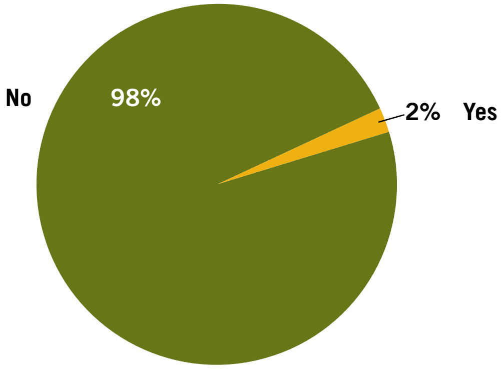


*Represents respondents who are aware of the PCI DSS

Brick-and-mortar retailers and micro-merchants cannot afford to remain behind in their efforts to understand and apply the PCI DSS. Free-form responses indicate that some merchants within the micro-merchant group feel the PCI DSS is too complicated or unattainable for their operation size, while those in the B&M merchant group express confusion surrounding their business model and PCI's applicability. In both cases, additional assistance is needed from ISOs and acquirers.

DETAILED FINDINGS AND COMMENTARY:

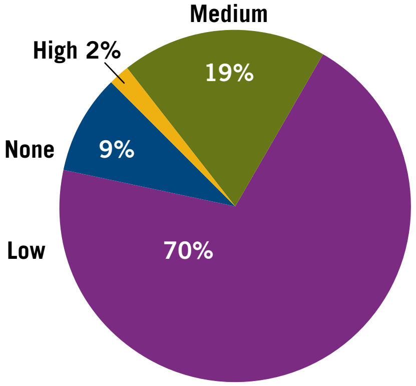
1. Has your company ever experienced a data breach?



Overall, 2% of this year's respondents said they had experienced a data breach. Merchants may not view that as an alarming statistic, and may even feel a certain sense of security because breaches are relatively rare events; however, merchants should be considering how, or even if, they could recover should a data breach happen to them.

The Verizon 2012 Data Breach Investigations Report discusses the connection between successful PCI compliance validation and data breach incidents: 96% of last year's breach victims were not PCI compliant. In addition, the report reviews a "continuing trend whereby more of the organizations that fall in the 96% tend to be on the small side—a shift toward Level 4 merchants. In many cases, these organizations have either failed to perform their (self) assessments or failed to meet one or more of the requirements."

2. In your opinion, how big of a risk does your company face from a data compromise?



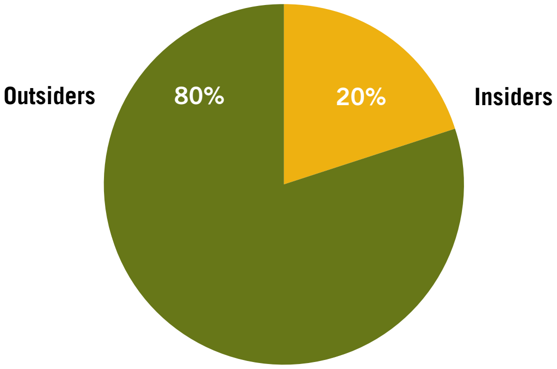
Nearly 80% of the respondents felt they had no risk or very low risk of a data compromise happening to their business. This finding is consistent with responses from previous years. The high overall percentage of the number of merchants with the "it can't happen to me" attitude indicates that not enough Level 4 merchants truly grasp the gravity of a data breach.

A single data breach can result in major business disruption and catastrophic financial losses. Survey respondents who have experienced a breach—and survived to talk about it—are now taking a stronger, more realistic stance with regard to PCI DSS compliance and data security. For example, they no longer see themselves at "high risk" for another data breach incident (most likely due to their extensive remediation efforts following the previous breach); however, they don't consider themselves to be at the "no risk" level either. Those merchants who haven't yet been breached still have the opportunity to proactively address their security before their livelihood is potentially compromised (given Visa data showing that Level 4 business breaches are on the rise).

RESPONDENTS' COMMENTS

"Small businesses under $15 million in sales should not have to jump through the same hoops as the big guys. Threat level is very low and compliance is very costly."

3. Whom do you see as the greater threat to payment data security, outsiders (e.g., hackers or criminals) or insiders (e.g., employees)?



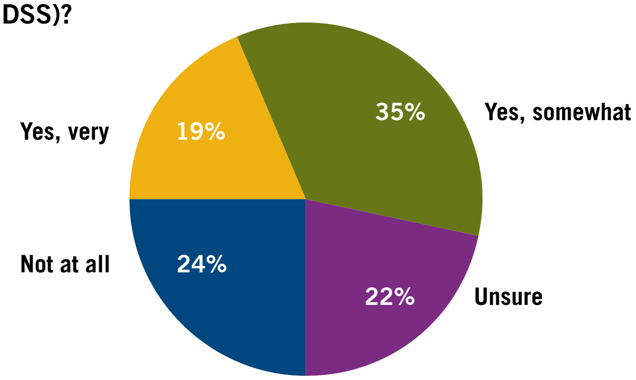
Overall, Level 4 merchants are much more concerned about outsider threats to data security than employee-driven breaches. When examining larger Level 4 merchants, however, it's not surprising that their perceived risk of internal threat is 22% higher than the group average.

RESPONDENTS' COMMENTS

"I am the only person in this hair salon and it seems unfair to add a PCI Compliance fee to someone that has regular clients with no employees and no one having access to any personal information other than myself."

It's logical that the greater the number of employees (especially those with access to company systems), the greater the chance someone will make an error that allows unauthorized data access. Conversely, many micro-merchants, especially family-operated businesses, feel that the PCI DSS unnecessarily forces them to guard against unlikely "inside jobs." This perception of inapplicability may contribute to a checked SAQ box with no accompanying action.

4. Are you familiar with the Payment Card Industry Data Security Standard (PCI DSS)?

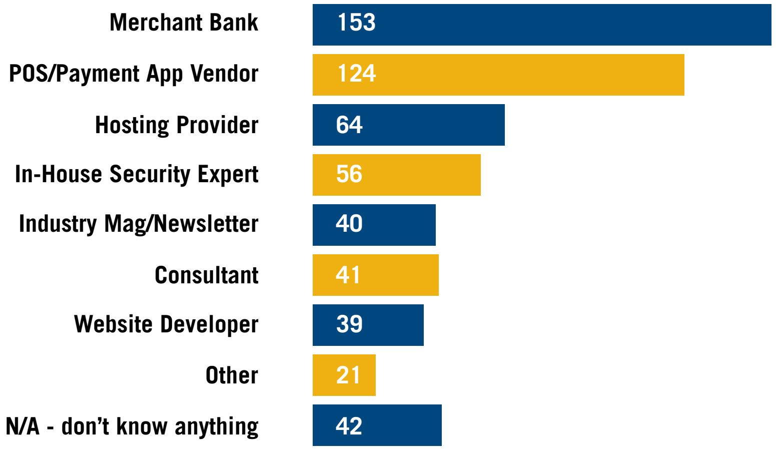


Familiarity with the PCI DSS is virtually unchanged since last year's survey. Awareness continues to be highest among ecommerce merchants (67%) and companies with 51 or more employees (77%). Awareness is lowest among B&M retail stores (51%).

The survey results show that all categories of Level 4 merchants need more PCI education. Not only is the Level 4 payment environment a concern, but also small merchants' growing reliance upon the Internet in general. The 2012 National Small Business Study found that 71% of the small businesses they surveyed utilize the Internet within their day-to-day operations and that two-thirds of respondents are more dependent on the Internet today than they were one year ago. This is significant, because all Internet-facing systems and applications are susceptible to breach—an issue that most small merchants seem to be unaware of.

The remaining survey questions were completed by only those with some familiarity of the PCI DSS.

5. To whom do you consult to learn about data security and PCI compliance? Check all that apply.



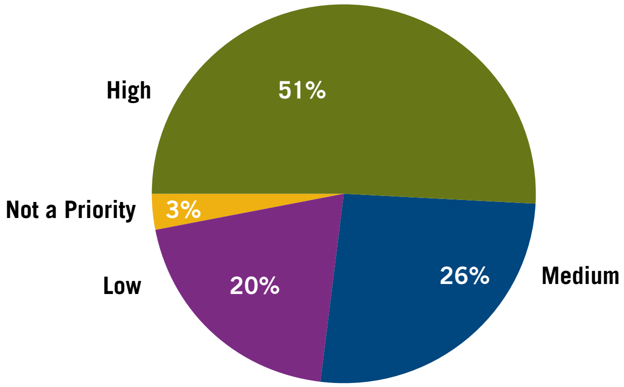
RESPONDENTS' COMMENTS

"I have no idea of the details. I rely on my credit card processor and POS software support people to be the experts and take care of it."

Level 4 merchants rely on a variety of parties for advice on data security and PCI compliance. Many consult with more than one entity. These consultative organizations are vital for successful understanding and compliance with the PCI DSS—and ultimately, for the survival of many Level 4 merchants who could be victimized without solid leadership from their advisors.

Merchant banks (i.e. ISOs and acquirers) still lead as the most utilized information source. Other oft-chosen advisors are POS/payment application vendors (35%) and hosting service providers (18%).

6. Where does data security fall in terms of your overall priorities?

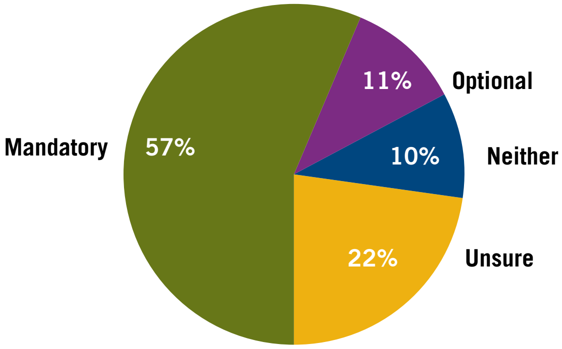


This year, 77% of respondents ranked data security as a "high" or "medium" priority, down from 83% in 2011 and 84% in 2010. Ecommerce merchants and those with more than 50 employees indicate they place a higher priority on security (79% and 96% for 2012 responses, respectively).

Even though, overall, more than three-quarters of merchants place some importance upon improving or maintaining data security, other survey responses indicate that there is little actual activity supporting these assertions.

For example, responses to Question 9 reveal that many merchants do not understand how to comply with the PCI DSS. Also, in Question 13, a number of the merchants who have validated PCI compliance admit they "just completed the paperwork," suggesting a lack of understanding regarding the activities that go along with making security a priority.

7. Is PCI compliance mandatory or optional for your company?



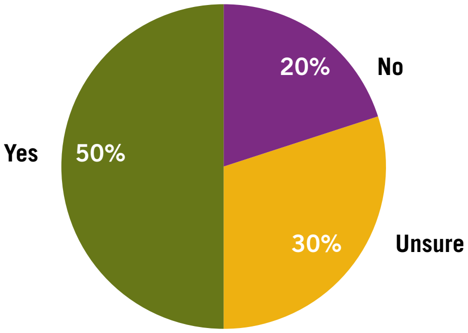
RESPONDENTS' COMMENTS

"Placing the onus for securing customer card data entirely on merchants is unrealistic. Cardholders should be provided with additional options to secure and approve/deny their own transactions."

This question is meant to gauge surveyed merchants' awareness that their business is subject to the PCI DSS. As might be expected, responses to this question by merchant group vary considerably.

Respondent groups with the highest "mandatory" answers are ecommerce firms (70%) and companies with 51 or more employees (82%). In contrast, 52% of B&M respondents realize that PCI compliance is mandatory for their business. Responses from those who are unclear or unaware of the PCI compliance mandate indicate that small business owners are most likely not sharing important security information with their staff or are simply unaware themselves.

8. Have you validated that you are PCI compliant?



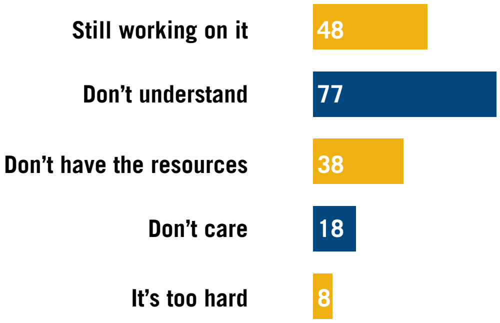
RESPONDENTS' COMMENTS

"I do have all that paperwork. I think these sorts of things are pretty confusing for a one-person small business."

Of those respondents who are aware of the PCI DSS, only half say they have validated their business's compliance—a drop of 7% from last year's reported results.

Another source of concern: 30% of respondents are "unsure" whether or not they have validated compliance, and the percentage climbs to 35% for brick-and-mortar businesses. This self-reported lack of awareness underscores the obvious need Level 4 merchants have for outside assistance to understand and meet PCI DSS requirements.

9. [If the response to Question 8 was No:] Why haven't you completed the PCI compliance process? Check all that apply.

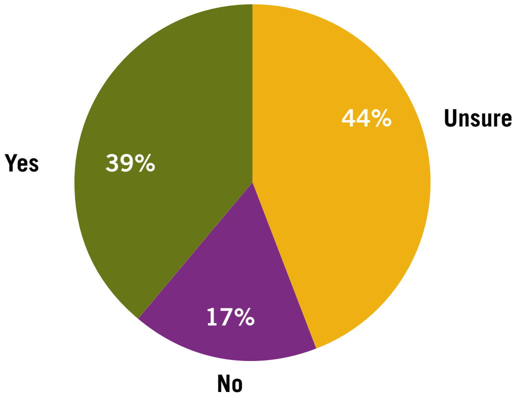


RESPONDENTS' COMMENTS

"I'm unclear as to what PCI Data Security entails. Please explain to help me make an educated decision. Thank You."

Larger Level 4 merchants stand out in the year-over-year analysis, indicating that for the most part they have either already validated compliance or are "working on it." The overall respondent group also demonstrates that they care about ensuring their customers' security, but they also indicate a need for additional education and assistance. In most cases, these small merchants simply don't understand how to complete the process and/or don't have the expert resources to help them through it. What these merchants need is simplification, so they can stay focused on the day-to-day activities that make their business profitable.

10. If you were to experience a breach and were PCI compliant, would you have the documentation to support your PCI compliance Self-Assessment Questionnaire?



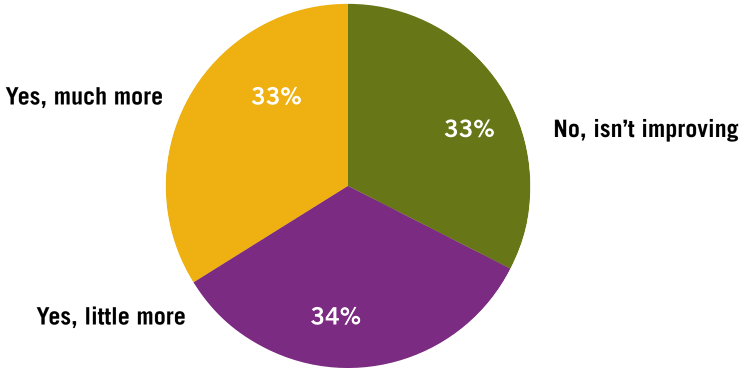
Only 39% of PCI-validated respondents claim they have the documentation to support their SAQ responses—a decline of 8% since 2011, and a reset back to the 39% seen in 2010. The lack of documentation is much more prevalent for B&M retailers (69% don't have it, compared to 40% for ecommerce retailers).

RESPONDENTS' COMMENTS

"Seems confusing. I believe we are 100% [compliant] but sometimes feel unsure."

Perhaps some merchants aren't taking the compliance process seriously and are simply "checking the boxes" of the SAQ. Others, bewildered by the process, are unclear on what practices make them compliant (or non-compliant) and simply hold out hope that they are.

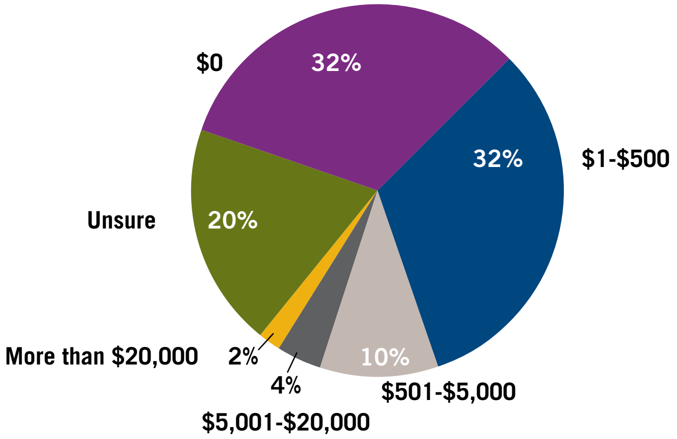
11. Do you believe that complying with the PCI standard will help your business become more secure?



For three consecutive years, the findings from this question have been identical: Two-thirds of respondents agree that PCI makes their businesses more secure.

The perceived futility of the 33% who don't believe they have achieved a higher level of security from PCI compliance further demonstrates the considerable challenge ISOs/acquirers face as they work to minimize breach-related risk within their merchant portfolios. Thankfully, a growing body of industry research (referenced within various sections of this report) reinforces the position that adherence to the PCI DSS does in fact decrease the Level 4 merchant's risk of breach.

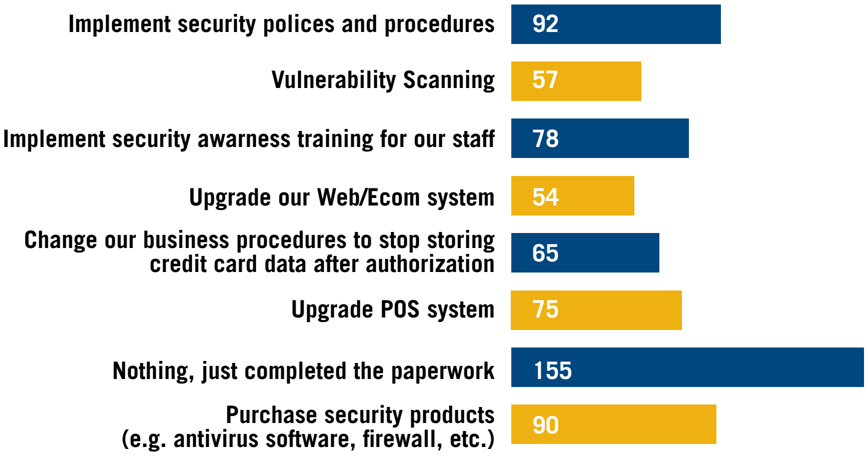
12. How much have you spent to achieve PCI compliance?



In 2011, we saw a year-over-year increase in Level 4 merchant spending on PCI compliance-related activities and technologies. This year there was a slight decrease, from 51% of respondents investing money toward PCI compliance in 2011 to 48% in 2012. An examination of B&M retailers' responses reveals that their spending also trends on the same year-over-year pattern (39% in 2010, 50% in 2011 and 45% in 2012).

A zero-dollar annual spend on PCI compliance can indicate that the merchant doesn't realize an investment is required to achieve compliance. In all years studied, micro-merchants made up the majority of those indicating a zero-dollar spend (43% in 2010, 31% in 2011 and 36% in 2012).

13. What did you have to do or purchase to meet PCI compliance guidelines? Check all that apply.



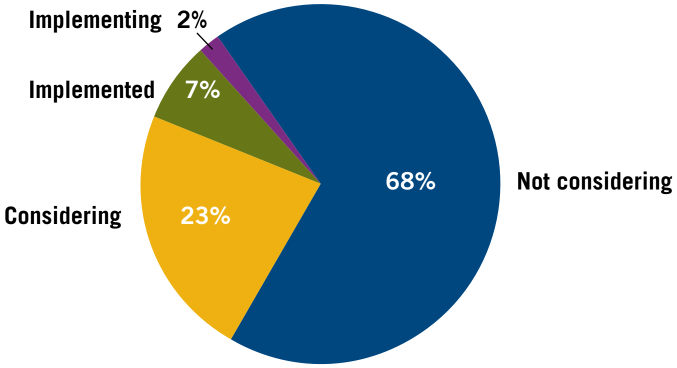
By far the most popular answer chosen for this question continues to be "Nothing, just completed the paperwork." Overall, 43% of respondents chose this answer in the 2012 survey. While this number is down from 48% in 2011, it still highlights a major gap in Level 4 merchants' understanding of what's required of them in order to truly be PCI compliant.

RESPONDENTS' COMMENTS

"As an end-user, I would like the process to be invisible to me and easily obtained via our vendors handling the transactions."

If the merchant did or purchased nothing to validate compliance, it most likely means they did not effectively meet the PCI DSS guidelines, because annual compliance validation almost always requires some type of action. Most merchants are required to put security policies in place and conduct internal security awareness training; security policies and internal training often come standard with most reputable PCI programs, at no additional cost to the merchant.

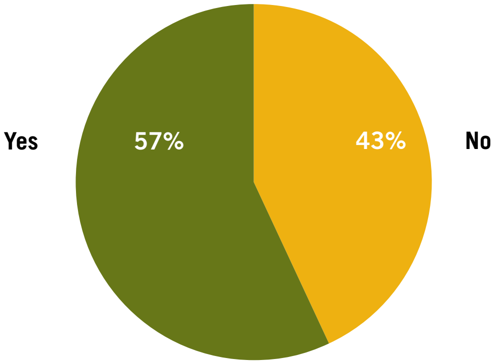
14. Have you considered end-to-end encryption or tokenization solutions to help reduce the scope of your PCI compliance efforts?



More than two-thirds of respondents have not implemented, and are not yet considering, end-to-end (E2E) or tokenization technologies to enhance data security. This number has not changed since the question was first posed in 2010.

Encryption and tokenization are effective technologies for enhancing data security, and the PCI Security Standards Council (SSC) is putting measures in place to help merchants wishing to adopt this technology select the solution providers who make security a priority. Free-form survey responses indicate a general lack of knowledge about these and other data security technologies. The ControlScan Acquirer Study found that only half of acquirers are offering or helping merchants select these services, which may partially explain the low awareness and adoption rate.

15. Do you think the PCI standard should apply to your business?



Of merchants with some awareness of PCI, the majority (57%) think it should apply to their business; however, a fewer number of B&M merchants (54%) and micro-merchants (also 54%) believe this to be true. With just over half of Level 4 merchants grasping PCI well enough to see its value for their business, it's clear that action needs to be taken to convince them that it is in their benefit. The 43% of merchants who say PCI shouldn't apply to them are going to be a tough sell; however, the industry research cited within this paper demonstrates the necessity of stronger Level 4 merchant communications and support.

16. What would you like to see changed or enhanced to the PCI Data Security Standard?

This free-form question encouraged respondents to "speak their minds"—and many did. On an encouraging note, the most frequent response to the question above was some variation of, "Do nothing. It's fine as it is."

Here are some of the other common themes among the responses, which aptly reflect the mindset of the small business owner:

- More clarity and simplified language,
- Streamlined requirements, education and tools, and
- Affordability through less unnecessary services, rules and fees.

RESPONDENTS' COMMENTS

"Make it understandable. Make it accessible for the small and very small business. Provide resources for applying the standards to particular business needs."

RESPONDENTS' COMMENTS

"Make the rules easier to understand. It's written in lawyer and tech language."

Level 4 merchants have the steepest learning curve when it comes to the PCI DSS and data security, and within that group, there are sub-groups with additional challenges. For the micro-merchant, it's understanding why they need to be so vigilant when they are the only one (or one of a very few) running the show. For the brick-and-mortar retailer, the primary challenge can be coming up to speed with how their payment system could still be compromised, even when their POS vendor assures them it's secure.

Level 4 merchants simply need more context to understand how all this applies to them. And, the ISOs and acquirers serving them need to have a program in place to support them every step of the way.

RECOMMENDATIONS FOR ISOs AND ACQUIRERS:

Merchants' overall inaction with regard to data security matters is completely understandable. Most small (Level 4) business owners are founders, entrepreneurs or front-line managers. They are extremely busy with operations, finance, sales, marketing and the other aspects of running a small business. They have little time, inclination or technical expertise to focus their attention on data security. With many distractions in place, merchants are prone to viewing PCI compliance as a "test"—an unavoidable check-off item that needs to be dispensed with quickly.

ISOs and acquirers can provide high value by moving into this void and offering leadership to frustrated, confused merchants. By elevating their awareness of the financial consequences associated with non-compliance—and offering ongoing services to help protect their business against a potentially catastrophic data breach—ISOs and acquirers will open doors to stronger, long-term relationships with their customers.

Here are four recommendations directed specifically at the ISO and merchant acquirer, to help them grow in their role as a vital merchant partner.

1. Mine customer data to create risk-based action plans.
There are many indicators of high-versus-low risk to look for with regard to Level 4 merchants. A great place to start is the MCC, or Merchant Category Classification. Some codes to watch for are those within the 5800 range, which represent restaurants. According to a recent Visa webinar, restaurants represent the highest level of merchant risk based on breach history. Visa data show that other high-risk categories include lodging/hotels, miscellaneous and specialty shops, direct marketing firms and clothing retailers.

Another merchant data point to examine is transaction volume. Seasonal merchants with lower annual transaction averages are lower risk than merchants with a high volume of transactions from year-round credit card sales. Merchants using dial-up terminals also represent a lower risk than those who use Internet-connected card processing methods.

ISOs and acquirers should make every attempt to know their merchants' primary service providers and monitor their compliance status and reputation in the marketplace, all the while encouraging merchants to use payment applications that are PA-DSS validated.

2. Strengthen communications with the riskiest merchants.
While all merchants must be PCI compliant, it can be beneficial to focus validation efforts on the riskiest merchants first, sending frequent messages that educate and reinforce urgency. As evidenced throughout this report, merchants have an unfulfilled need for additional information on how to effectively secure cardholder data and meet PCI compliance requirements. They are looking to ISOs and acquirers for this information, as well as cost-effective solutions for streamlining their security-related processes.

Many small merchants do not understand why the PCI DSS should apply to them. It's important to specifically reach out to these merchants with information surrounding the basics of PCI, why it applies to them and the tangible business risks of non-compliance. The first step is to build a foundation of awareness so that future messages relating to compliance do not go unnoticed. A multi-channel communication approach (e.g., statement messages/inserts, email, direct mail, outbound calls, etc.) is also recommended to facilitate merchant engagement.

Frequent, targeted communications will build understanding and goodwill with merchants. In addition, regular outreach will drive message retention and the appropriate merchant action.

3. Equip merchant-facing representatives with the right tools.
Some ISOs and acquirers prefer to wholly manage their PCI program while others outsource this activity to a specialty provider. Regardless, the ISO/acquirer organization should maintain complete visibility into the program's activities, including merchant communications and support events. This level of visibility ensures that the organization is properly monitoring individual merchant engagement with PCI. In addition, all merchant-facing staff should be well informed about the program and the basics of PCI compliance so they can provide a consistent message to merchants.

It's also recommended that ISOs and acquirers synchronize merchants' PCI compliance status with their company database, so customer service personnel have easy access when interacting with merchants. Then, when a representative has a merchant on the phone, they can be more knowledgeable and proactive with their advice, encouragement and engagement in the PCI compliance process. This type of data integration is also useful for producing actionable reports or informing decisions to adjust the PCI program and related communications.

4. Offer technology and service solutions to solve merchants' problems.
As competition within the merchant services space continues to intensify, a goal of every ISO and acquirer should be to offer solutions that help simplify merchants' PCI compliance process, reduce their overall scope and secure their business in an affordable way. This involves understanding merchants' security needs and any gaps they may need help filling, as well as aligning with the right partners who have experience in and are committed to helping small businesses. Level 4 business owners will find tremendous value in this, since they rarely have the necessary technical and security resources in-house, nor do they have the budget to afford enterprise-level solutions.

The partnering approach bolsters the ISO/acquirer solution set, expanding their reach as well as merchants' perceived value of the overall business relationship. Partnerships can connect Level 4 merchants with helpful services such as security awareness training, managed security services and penetration testing, as well as end-to-end/point-to-point encryption and tokenization solutions. The PCI SSC website and established industry connections are great resources for discovering companies with the specific credentials and tools that can help small business owners. ISOs and acquirers can either recommend partners directly to merchants or include partner services as part of their own security management toolbox.

PCI Compliance: Helping small merchants cross the chasm

The last four years have been marked by continued growth in small business data compromise, yet Level 4 merchants are still working toward the same not-so-simple goal, which is to run a profitable business. Both ecommerce and brick-and-mortar merchants need hands-on support to simplify PCI compliance and ongoing data security; this business need presents an important opportunity for ISOs and acquirers to build relational value with their primary customers. The ISOs and acquirers who understand and address awareness-and-action gaps with personalized, knowledgeable service and scalable, cost-effective technology offerings will become the small merchant's provider of choice.

ABOUT THE SURVEY SPONSORS:

ControlScan:

Headquartered in Atlanta, Georgia, ControlScan is the leading provider of Payment Card Industry (PCI) Compliance and Security services designed to meet the unique needs of small to mid-sized merchants and the acquirers that serve them. The company's flexible solutions, easy-to-use online tools and personalized support significantly simplify PCI and security for its clients. In addition, as an Approved Scanning Vendor and a Qualified Security Assessor, ControlScan is positioned to help merchants meet compliance requirements and maintain secure business environments for their customers. For more information about ControlScan and its cloud-based solutions visit www.controlscan.com or call 1-800-825-3301.

Merchant Warehouse:

Merchant Warehouse is a recognized leader in payment and program acceptance solutions and merchant services. The company enables merchants, agents, POS developers and VARs to achieve strategic business advantage through the delivery of current and emerging payment, offer and program solutions and merchant services that dramatically enhance the merchant-customer experience. Merchant Warehouse is one of the fastest growing innovators of payment solutions in North America. For more information about Merchant Warehouse, please visit merchantwarehouse.com or follow the company on Twitter at http://twitter.com/MWarehouse.