What Small Merchants Know (and Don't Know) about PCI Compliance

A Research Report
August 2009

ControlScan™ Security that fits.

National Retail Federation® The Voice of Retail Worldwide

pci knowledge base

Executive Summary

When hundreds of thousands of cardholders are affected by data breaches at big box retailers, the public hears about it.

Far less sensational, but equally serious consequences occur when there's a data compromise at a small retailer. When a local repair shop or an online boutique is compromised, the national media doesn't report the story so you don't learn that a data breach was the proverbial "last straw" for the owner. She had fire insurance and premises liability insurance, but she never knew that a hacker could put her out of business.

In spite of valiant efforts to keep PCI compliance relatively simple, large numbers of small and mid-sized merchants (Level 4 as defined by Visa) are somewhat bewildered by the Payment Card Industry Data Security Standard (PCI DSS). The standard is meant to keep their customers' data safer but understanding it has proven difficult for small merchants.

That's only one of the major findings of a survey of 220 small merchants conducted in July 2009 by ControlScan, the National Retail Federation (NRF) and the PCI Knowledge Base.

A key implication of the survey: acquirers, ISOs and other providers serving the industry need to stand up, exercise leadership and guide merchants along the path to compliance. In fact, the survey indicates that small merchants look first to these organizations for leadership and guidance in this area.

Another key finding is that until industry service providers and the PCI Security Standards Council make PCI compliance easier to understand and less complex to implement, many small merchants will likely continue to suffer data breaches because they are not taking the requisite steps to properly secure their customers' data.

With the survey, ControlScan, the National Retail Federation and the PCI Knowledge Base set out to gain broad insights into Level 4 merchants and their status with PCI Compliance.

Specifically, the goals of the study were to determine:

- Merchants' awareness, understanding and acceptance of PCI DSS.
- Their perception of the risks associated with a data breach.
- How well they think they are doing regarding compliance.
- What they are spending on compliance.

The findings are based on survey responses representing all types of ecommerce, retail store and mail order/telephone order (MOTO) merchants. Overall, the study revealed some good news and some bad news for ISOs, acquirers and other industry service providers.

The good news: Awareness of PCI compliance and perceived value in securing customer data is high.

The bad news: The level of understanding about PCI and how to comply with PCI DSS is not high.

This report first presents high-level "takeaways," followed by the detailed survey findings and their implications. The study concludes with recommended actions ISOs and acquirers can take to help their small merchant portfolio maintain a high security posture.

Methodology and Audience Profile

The online survey was conducted in July 2009. Respondents were randomly selected from the databases of:

- ControlScan, the leading provider of PCI compliance and security solutions exclusively designed for small merchants.
- The National Retail Federation, the world's largest retail trade association.
- The PCI Knowledge Base, the largest independent research community focused on the security of payment and related financial and personal data.

This survey resulted in 220 responses. Of the 220 respondents, 83% said they are familiar with Payment Card Industry Data Security Standard. In questions 4 through 13, only this group of 182 positive responses is tabulated. (The identical number, 182, of respondents answered "Yes" to the question, "Does PCI apply to your business?")

Respondents supplied profile information. Highlights are as follows:

- Merchant types include ecommerce, retail store and MOTO categories. 45% of the merchants operate in more than one of these categories.
- More than half of the respondents are CEOs, Presidents or Owners (most likely the principals of small-to-mid-size businesses or sole proprietorships).
- 57% of the merchants have one to ten employees.
- 45% of the merchants get 100% of their business from Card Not Present (CNP) transactions.
- Almost half (48%) of the respondents process fewer than 100,000 annual credit/debit card transactions.
- For 89% of the merchants, the average sale is between $10 and $1,000.

Key Takeaways

- While the PCI DSS has been around for several years, it has just recently started to resonate with Level 4 merchants. This trend may be largely due to acquirers and ISOs mandating compliance within their merchant portfolios. Over the past 12 months, there has been a considerable uptick in the number of acquirers and ISOs that are requiring small merchants to demonstrate compliance with the PCI DSS.
- Less comforting is the apparent low appreciation by small merchants of the risks of a data breach. It's human nature to ignore or avoid matters one doesn't understand, and that could be the root cause of the dichotomies revealed by the survey:
  - High awareness of PCI and a strong belief that it is important.
  - High frustration with understanding, implementing and paying for compliance.
  - Low concern about the risks of compromised data, except for those that have already been breached.
- Merchants say they see value in PCI compliance. They are predisposed to act if providers show them how their value-based services will help them achieve compliance.
- Merchants look to banks, acquirers, ISOs, and other payment processing vendors as their "go to" resources for PCI compliance and security information. Respondents' free-form comments repeatedly implore the industry to make compliance easier and simpler.

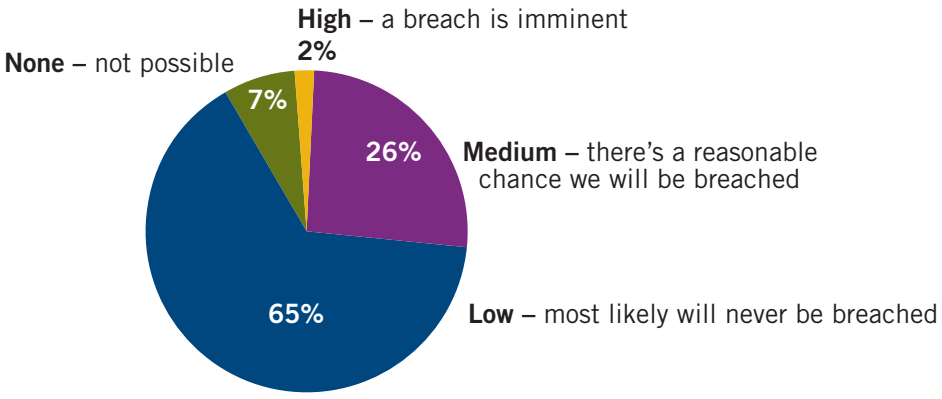
RESPONDENTS' COMMENTS

"We want to comply, but we're not IT gurus. Please educate us and make it clear what we need to do. Help us to make compliance as simple and practical as possible."

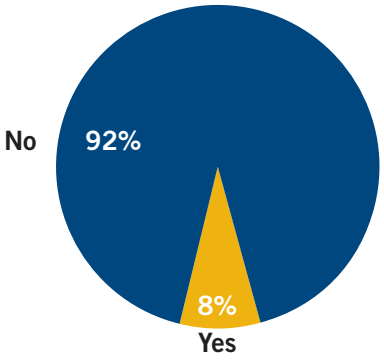
DETAILED FINDINGS AND IMPLICATIONS

Data Breaches

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



2. Has your company experienced a data breach?

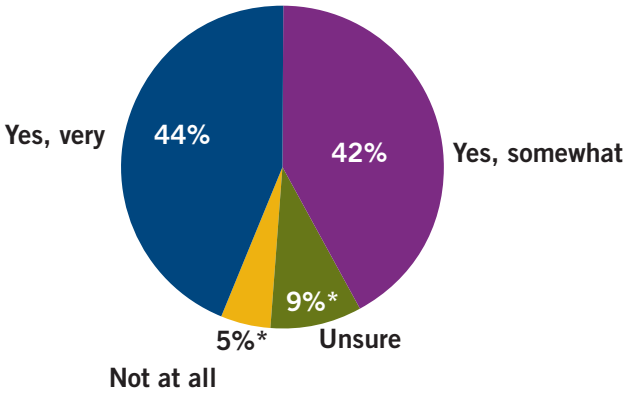


Implications: Responses to these two questions suggest that respondents don't understand the severe consequences or the risks resulting from a data breach. The reported data breach rate of 8% among respondents may seem small—but actually is quite high compared to the incidence rates of other hazards that merchants are familiar with, such as fire or water damage. On the other hand, 92% of respondents consider the risk of a data compromise to be low or nil.

These findings suggest there is a disconnect between merchants' perception of low risk and the reality of a relatively high incidence rate. However, this changes significantly if merchants have already been breached. In that case, nearly 70% of breached respondents considered the risk of a data compromise to be high or medium. Clearly, small merchants need to be better informed of the potential costs and penalties they could incur from a data breach before it happens.

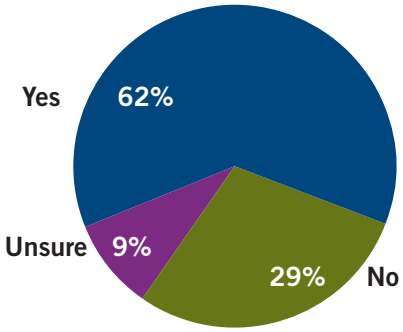
Understanding of PCI compliance

3. Are you familiar with the Payment Card Industry Data Security Standard?



* Responses from this group were not tabulated for subsequent questions

4. Have you validated that you are PCI compliant?



RESPONDENTS' COMMENTS

"Either make things easier to understand or offer more help for businesses to get compliant."

Implications: A year ago, industry observers say there was less awareness of the PCI standard. Now the picture has changed significantly, probably because various organizations are making validation of compliance mandatory. Today, small merchants say that they are aware of PCI DSS. Question 3 found that 86% of survey respondents claim to be somewhat or very familiar with the PCI standard. Yet, in Question 4, only 62% of respondents say they have "validated" that they are PCI DSS compliant.

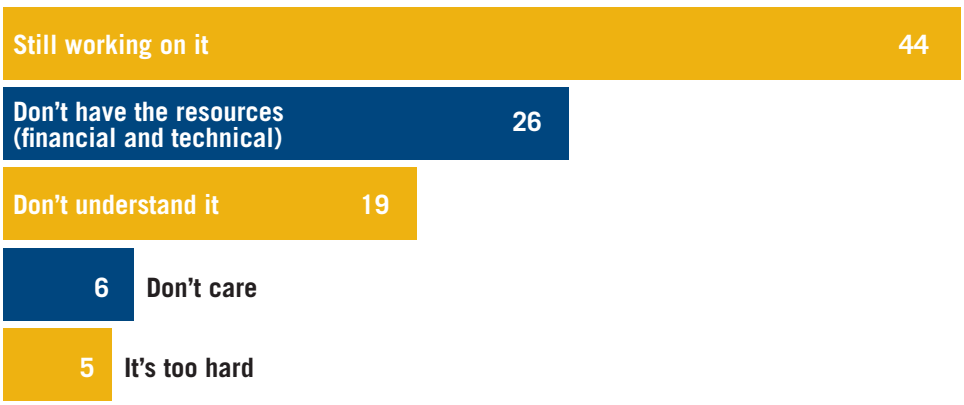
High awareness demonstrates that merchants are receptive to becoming PCI compliant. However, there is a significant performance gap—a 24% difference between their familiarity and the key action (compliance validation) that informed merchants would reasonably take. It is incumbent on the industry to help narrow the performance gap between merchants' awareness of PCI and their validated compliance.

RESPONDENTS' COMMENTS

"Make it easier for non-technical folks to understand."

Merchant education efforts need to focus on a tactical level. Merchants want to know specifically what has to be done and the easiest, least expensive route to completing the compliance process.

5. [If the response to Question 4 was No:] Why haven't you completed the PCI compliance process? Check all that apply. (in order of # of responses)

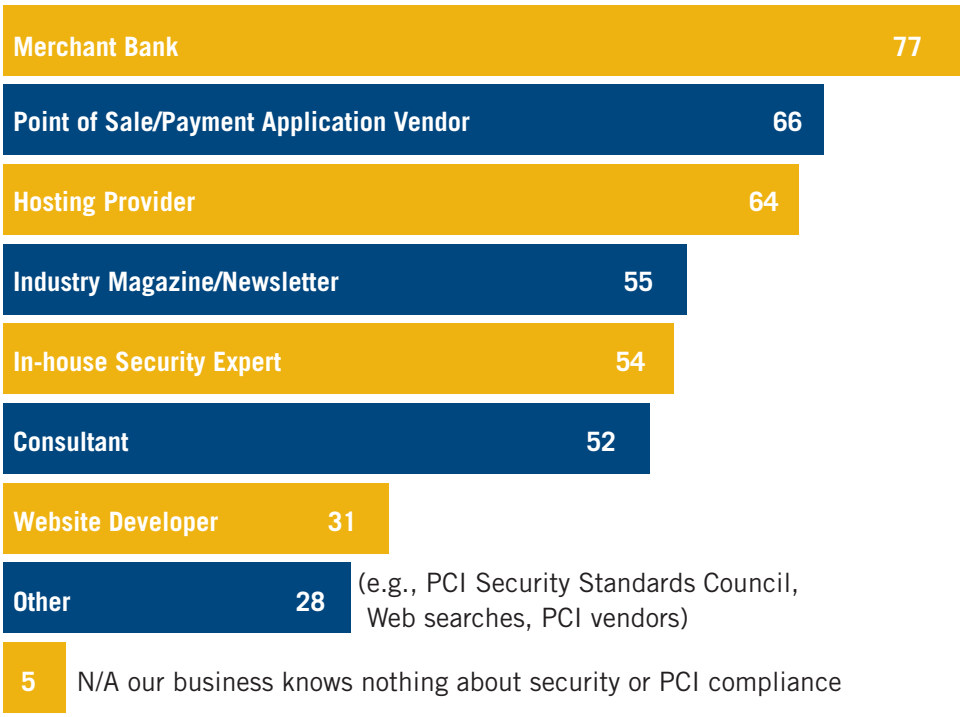


RESPONDENTS' COMMENTS

"Much greater clarity is needed. Also a number of items on the questionnaire make little or no sense in the context of a small business with few employees."

Implications: The respondents who are not compliant gave one or more reasons for not completing the process. The reasons cited—particularly "don't understand it," "don't have the resources," and "too hard"—suggest that merchants are crying out for help in a matter that frustrates them. Acquirers and ISOs have an opportunity to step up and offer a helping hand to these befuddled merchants, as well as those who have checked the boxes but don't really understand the commitment they are making or the technologies involved.

6. To whom do you consult to learn about data security and PCI compliance? Check all that apply. (in order of # of responses)

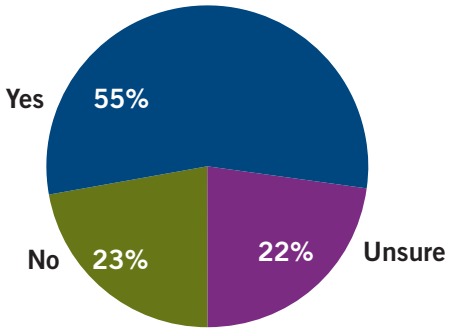


RESPONDENTS' COMMENTS

"I think PCI standards should be checked by the merchant banks for the business owner. We are not experts in credit card security."

Implications: Educating customers is a hallmark of leadership. Small businesses first look to their banks and then to vendors of point-of-sale software, payment equipment and hosting for guidance. These organizations are uniquely positioned to embrace their de facto "first responder" role in the PCI education arena. By assisting small merchants to become PCI compliant and providing them with easy-to-understand information that they can review in small doses, they can potentially gain market share and increase customer loyalty.

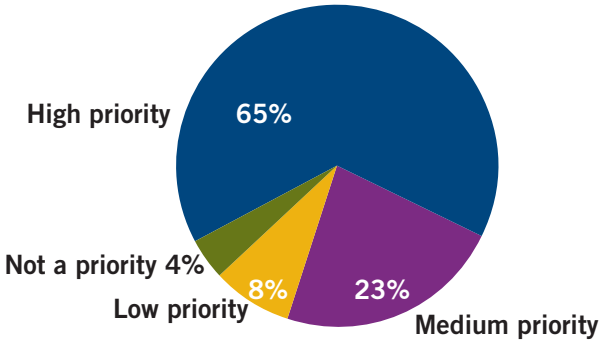
7. If you were to experience a breach and were PCI compliant, would you have the documentation to support your PCI compliance Self Assessment Questionnaire?



Implications: 45% say they can't demonstrate that they are compliant, which may imply that many small merchants are taking a "check the box" approach to compliance and security and then moving on to other initiatives. This is totally understandable and another reason why the industry must do more to facilitate PCI compliance and promote security as an ongoing process—not a single point-in-time event. For example, acquirers and ISOs may want to consider offering "templates" of the policies, procedures and forms that are needed, along with simple guides to help small merchants customize them.

Commitment to PCI compliance

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



Implications: For all merchants, 88% of respondents say data security is a "High" or "Medium" priority. It remains to be seen if they are indeed willing to act on these convictions—but this finding is yet another positive indication that there is demand for value-added compliance and security-related offerings from service providers.

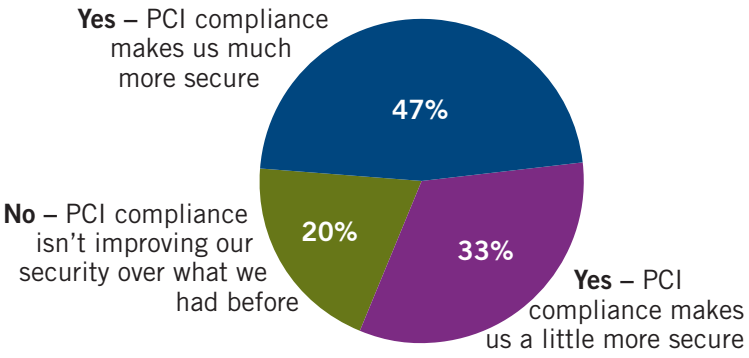
Cross analyzing these findings with other responses revealed some interesting insights:

- For five of six merchant types, PCI compliance was ranked as a "High" priority by at least 67% of respondents. But the retail-only type respondent was much less committed; only 30% ranked PCI as a "High" priority. This strongly suggests that "mom and pop" dry cleaners, pizza parlors and convenience stores still do not view data security, PCI or hackers as things they need to be concerned about. Changing this perception will require a concerted effort by ISOs, acquirers and retail POS resellers and anyone else who services small merchants.
- Among respondents that have experienced a data breach previously, 92% rank PCI compliance as a "High" priority—compared to only 63% for responses from companies that have never had a data breach. Understandably, a data breach is a "wake up" call.

RESPONDENTS' COMMENTS

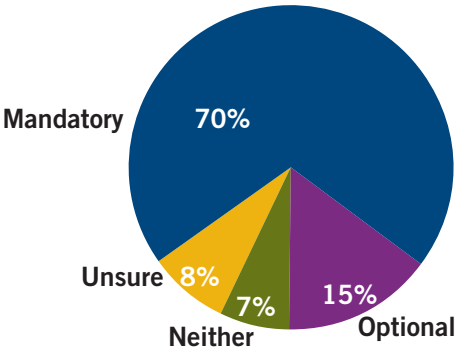
"Targeted education at the leadership level will accelerate acceptance and likely encourage appropriation of capital to security projects."

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

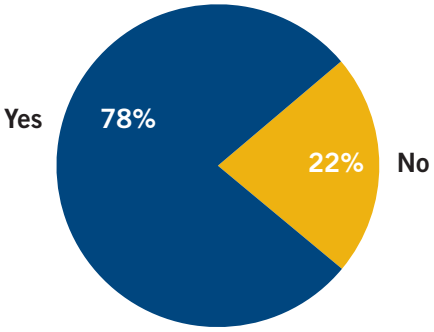


Implications: 80% of responses believe that PCI compliance makes them more secure. This positive finding, which is tightly coupled with Question 8's finding, further validates that at least some types of small merchants believe PCI compliance is important.

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



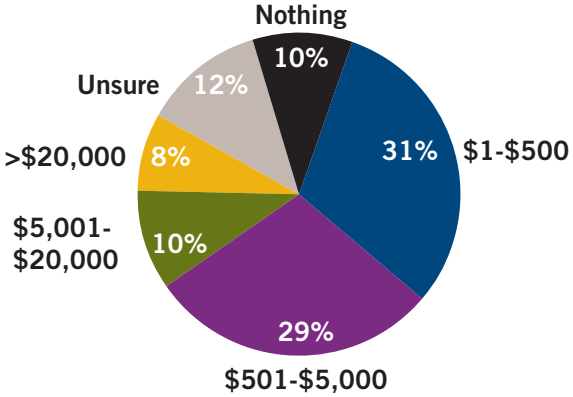
11. Do you think the PCI standards should apply to your business?



Implications: Industry participants should be pleased with these findings. Industry messages are beginning to work and creating some urgency around the theme that small businesses must be compliant. Merchants feel there are imperatives for them to be compliant, so they are predisposed to take actions to achieve compliance. It is important to note, however, that many more merchants believe PCI is both important and mandatory than are taking action to become compliant. So even when there is awareness, many merchants lack the resources or motivation to actually become compliant.

Costs of PCI compliance

12. How much have you spent to achieve PCI compliance? (182 responses)



RESPONDENTS' COMMENTS

"Better understanding of how much small businesses' can afford. Most solutions available are for large businesses and are expensive."

Implications: A good indicator for a reasonable spend level could be based on those merchants that truly take security and PCI compliance seriously. For example, among respondents who have experienced a data breach (Question 2), 69% spent $501-$5000 for compliance. Among merchants that have not been breached, only 26% reported the same level of spending.

Small businesses with few resources may be prone to cut corners on costs, especially when they don't understand the risks and the consequences. This is the security equivalent of buying fire insurance after a fire.

13. What did you have to do or purchase to meet PCI compliance guidelines? Check all that apply. (in order of # of responses)

RESPONDENTS' COMMENTS

"More information on scan reports on how to mitigate reported threats."

RESPONDENTS' COMMENTS

"A better description of what is expected to be implemented to comply."

RESPONDENTS' COMMENTS

"Better clarification and examples on how to apply each requirement."

Implications: The diversity of the actions small merchants are taking indicates that they are receptive to making the changes needed for PCI compliance. Of the nine choices presented in Question 13, most are easy steps to achieving compliance and do not require a large investment. Merchants know they need these services and they see value in having them performed. ISOs and acquirers also have an opportunity to encourage small merchants or provide services to help them avoid storing credit card data, which will make the requirements of PCI much easier to achieve and help curtail risk.

What ISOs and Acquirers Can Do Now

Based on the results of this study, there are some clear directives for the industry to further compliance among Level 4 merchants.

Here are five recommendations:

1. Be a leader. Merchants ranked banks and POS/payment consultants as their first "go to resource" in this area. It may seem awkward for a seller of services to also be an enthusiastic educator and missionary; but that's what merchants expect of firms they consider to be trusted advisors.

2. Keep it simple. Merchants have a foggy understanding of what they need to do to become PCI compliant because they are merchants, not security experts. Show the merchant a clear, practical, affordable path to success. Stay tactical.

3. Give your merchants jargon-free compliance guides and recommended security policies that merchants and their customer-facing employees can understand. Offer a robust PCI compliance service that is easy to use and will walk the merchant through the process in a step-by-step manner. If you don't have the resources, consider outsourcing your PCI compliance program to a company that will act as an extension of your team.

4. Advise merchants to avoid storing card data. Storing cardholder data after authorization requires a much more rigorous self-examination in order to become PCI compliant. (And it requires the business to answer 226 SAQ questions rather than 11-38 questions.)

5. Make sure your customers understand the risks and the costs of non-compliance. Tell them the harsh facts:

- 85% of payment card breaches occur at small businesses.
- 81% of organizations subject to PCI DSS had not been found compliant prior to the breach.
- 83% of attacks were not highly difficult to perform.
- Serious breaches can incur fines ranging from $5,000 to $25,000 every month until compliance is achieved. And that's on top of audit costs and loss of business if payment processing is halted.

About The Survey Sponsors

ControlScan:

ControlScan is the leading provider of Payment Card Industry (PCI) compliance and security solutions designed exclusively for small- to medium-sized ecommerce and retail merchants. ControlScan provides easy-to-use Web-based security solutions and a personal level of service that make it easy and cost-effective for these businesses to analyze, remediate and validate compliance. The company is also the solution of choice for small merchants and acquirers because it offers security solutions that are built specifically with the small merchant in mind, a personal level of service and the best results. Acquirers and other merchant service providers rely on ControlScan to manage PCI compliance programs for their entire merchant portfolios to ensure maximum compliance rates. For more information about ControlScan call 1-800-825-3301 or visit www.controlscan.com.

The National Retail Federation (NRF):

The NRF is the world's largest retail trade association, with membership that comprises all retail formats and channels of distribution including department, specialty, discount, catalog, Internet, independent stores, chain restaurants, drug stores and grocery stores as well as the industry's key trading partners of retail goods and services. NRF represents an industry with more than 1.6 million U.S. retail establishments, more than 24 million employees – about one in five American workers – and 2006 sales of $4.7 trillion. As the industry umbrella group, NRF also represents more than 100 state, national and international retail associations. www.nrf.com.

The PCI Knowledge Base:

The PCI Knowledge Base is the largest independent research community focused on the security of payment and related financial and personal data. The PCI Knowledge Base's registered membership includes over 2,800 persons who are focused on PCI, including retailers, hoteliers, academics, bankers, payment processors, PCI assessors (QSAs), providers of payment systems and security technologists. The company's panel of over 85 PCI Experts shares their knowledge and experience through its proprietary research database as well as through discussion forums and via our PCI Experts Blog. For more information call 214-295-4996 or visit www.pciknowleldgebase.com.