Risk and Revenue:

Second Annual Survey of the Acquirer's Perspective on Level 4 Merchant PCI Compliance

A Research Report
January 2013

ControlScan® PCI & Security That's Right For You.

MAC

Table of Contents:

Page:

Executive Summary:

PCI compliance goals shift away from risk and toward revenue as acquirers adapt to industry change.

This is an exciting and turbulent time in the payments space as industry-shaping initiatives and technology converge to produce dramatic change. The rapidly evolving payments landscape is challenging traditional merchant acquirers, including Independent Sales Organizations (ISOs), banks and payment processors, to re-evaluate their business models. At the same time, new entrants are exploring how technology can fuel a more efficient and profitable merchant-consumer dynamic.

From a payments security standpoint, acquirers are currently positioned at an intersection of the well-established Payment Card Industry Data Security Standard (PCI DSS) and conflicting merchant priorities. This is especially true for the Level 4 merchants they serve. Representing 98% of all U.S. retailers, these typically smaller-sized merchants process one to 20,000 online credit card transactions or one to one million face-to-face credit card transactions annually.

Level 4 merchants continue to show a lack of awareness and overall apathy toward PCI compliance and cardholder data security, yet they are facing a broadening threat landscape as data thieves exploit weaknesses in their processing environments. This, combined with card brand requirements surrounding PCI, presents an unusual challenge for acquirers: They are obliged to help merchants secure their business systems, but they also must effectively respond to competitive pressures that threaten merchant attrition.

Acquirers' PCI compliance programs are an important part of their overall business equation because they impact the relationships they have with their merchants, and because they reduce business risk that can affect their bottom line. As they establish the goals and strategies that will move their business forward, acquirers must take an introspective look at the components driving their Level 4 merchant PCI compliance program.

ControlScan and Merchant Acquirers' Committee (MAC) recently conducted their second annual survey of merchant acquirers, which was designed to measure acquirers' attitudes and objectives surrounding their Level 4 merchant PCI compliance program. The survey's results revealed several important trends, the most notable being that acquirers' PCI program goals have shifted from risk mitigation to revenue generation. This and other findings from the annual survey provide valuable insights into the acquirer's role as a payments industry stakeholder.

This research report examines this year’s survey responses from several angles, including acquirers’ business categories, portfolio sizes and reported compliance rates, to provide a comprehensive analysis of trends and disparities. The survey’s key findings are also discussed, along with their implications for acquirers and the greater payments community. The report concludes with acquirer-specific recommendations that should help them transform their PCI programs to create a stronger value exchange with the merchants they serve.

Methodology and Audience Profile:

The ControlScan/MAC Acquirer PCI Survey was conducted in October 2012, exactly one year after the inaugural survey that benchmarked acquirers’ perspectives on merchant PCI compliance. The most recent survey was once again sent to randomly selected ISOs, banks and payment processors 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 Acquirers’ Committee, an organization of bankcard professionals involved in the risk management side of card processing.

The latest survey was completed online by a total of 123 payment professionals. The population of responders had the following characteristics:

Audience profile by…	**Percent of responses**
Business classification:	
Bank	23%
ISO	49%
Processor	24%
Agent	2%
Other	3%
Size of Level 4 portfolio:	
<1,000 accounts	32%
1,001 – 5,000 accounts	24%
5,001 – 10,000 accounts	15%
10,001 – 50,000 accounts	14%
>50,000 accounts	14%

Ninety-six percent of respondents reported having a PCI program in place for their Level 4 merchants, representing a 2% increase from last year. Of these, the majority (59%) have now had their program in place for more than two years. The year-over-year data, presented in the following table, show the trend toward having PCI programs in place for a longer duration, reflecting the maturity of the PCI DSS within the payments space.

Duration of PCI program	2012 responses	2013 responses
<6 months	5%	6%
6 months-1 year	16%	8%
1-2 years	39%	29%
2-3 years	29%	30%
>3 years	11%	29%

The discussion in the remaining sections of this report involves the responses of the 96% who have a PCI program in place for their Level 4 merchants.

Key Findings:

An examination of this year's survey results found three areas of interest for the acquirers this report serves. These key findings provide an inside look into the differences between successful and unsuccessful PCI compliance programs, as well as the business drivers behind program trends.

Acquirers' PCI-related goals and strategies reflect a greater focus on revenue generation.

This year, responses to the survey question *"Please rank the goals of your company's PCI compliance program"* show a complete reversal from last year's responses, prompting another look at the goals and strategies driving acquirers' PCI compliance programs.

Please rank the goals of your company's PCI compliance program (1 is most important).

	2012	2013
Reduce risk resulting from breaches of cardholder data	1	4
Meet card brand requirements	2	2
Achieve high compliance rates	3	3
Generate additional revenue	4	1

Acquirers typically approach the PCI compliance process differently based upon their business category; however, this year’s results show an across-the-board selection of “generate additional revenue” as the number one PCI compliance program goal. The designation of “reduce risk…” as the lowest-level goal among the four underscores the significant divergence from last year’s responses.

This year’s survey results also reveal that acquirers are becoming more aggressive with PCI program fees. Responses to the question *“How much do you charge your merchants to participate in your PCI compliance program?”* indicate a widening divide in the way acquirers position their PCI compliance program to merchants:

- There has been virtually no change in the percentage of acquirers providing their PCI program at no charge to their merchants, but
- The percentage of acquirers charging an annual participation fee of $71 or more is on the rise, from 50% last year to 59% this year, and
- Eighty-three percent of acquirers with the lowest compliance rates charge the higher annual participation fee, versus 46% of those with the highest compliance rates.

The upward trend in PCI program participation fees, along with low-compliance acquirers’ slant toward the higher fee bracket, indicates that more acquirers could be using these fees for revenue generation versus strategic purposes.

To be sure, industry legislation, intensified competition and other economic influencers have reduced the contribution traditional merchant services make to acquirers’ bottom lines. As a result, acquirers are looking for opportunities to generate additional revenue through differentiated business offerings and programs.

Acquirers who make revenue generation a primary goal for their PCI compliance program will have a difficult time convincing already-wary merchants that they have their best interests at heart when it comes to PCI compliance and card data security. Like any consumer, merchants will require real business value in exchange for program participation fees. This value comes in the form of effective, easy-to-use assessment tools and solutions to help them remediate security gaps.

PCI-related goals can include revenue generation, but acquirers’ corresponding strategies must also involve value-added technologies and services that support merchants’ PCI compliance efforts, giving them the ability to focus more directly on their business. This combination will enable the acquirer to reap revenue-based rewards as well as risk reduction through a stronger merchant security posture.

Acquirers with organizationally-supported PCI programs achieve higher merchant PCI compliance rates *and* suffer fewer breaches.

At any given time, a financial organization can have multiple initiatives running in tandem toward achieving company and departmental goals. The initiatives that gain the most traction are those that are supported at an organizational level; therefore, when an organization's actions do not support a program's goals, the program is considered to have not achieved sufficient internal traction.

Survey respondents ranked organizational support for their PCI compliance program high on their list of challenges. In fact, a key finding of this year's survey is that as organizational support (i.e., internal traction) increases, so does the acquirer's merchant compliance rate.

The Relationship between Organizational Support and Merchant Compliance Rates

Of the acquirers reporting this level of PCI compliance achievement rates…	…this percentage said there is a "lack of traction" within their organization.
<10%	60%
11%-25%	38%
26%-40%	14%
41%-60%	9%
>61%	6%

The chart above demonstrates that 60% of acquirers reporting a PCI compliance rate of less than 10% feel their PCI program lacks traction within their own organization, while only 6% of acquirers with the highest PCI compliance rates report the same issue.

In addition to the positive relationship between organizational support and PCI compliance rates, there is also a continued correlation between PCI compliance rates and breach risk. Survey data from this year and last year confirm that those with compliance rates of 25% or less are more likely than those with compliance rates higher than 40% to have experienced a recent merchant breach.

Understandably, when compliance rates are high, acquirers are more likely to realize the value their PCI program brings to the organization as well as the merchants they serve. A solid 85% of acquirers reporting compliance rates of 61% or higher believe their PCI program has helped protect their merchants from breach, and 58% of those same acquirers feel that their merchants also see the benefit their PCI program provides.

Low merchant PCI compliance rates and perceived non-value are hallmarks of an ineffective PCI compliance program.

One quarter (26%) of this year's survey respondents reported a PCI compliance achievement rate of 25% or less. While this may seem like a relatively small segment of the overall respondent group, it is important to note that these acquirers share several characteristics that—when taken as a whole—are representative of an ineffective PCI compliance program.

The following common characteristics define acquirers with low merchant compliance rates:

- **Their merchant communications don't trigger action.** Acquirers with the lowest merchant compliance rates claim they are using just as many communications channels, with similar frequency, as their counterparts; however, the disparity in compliance rates indicates that their communications are ineffective in driving merchant action. A possible culprit may be insufficient communications during the merchant boarding process, or the acquirer's communications may not be reinforcing PCI's significance in the overall health of the merchant's business.

- **Their "added value" merchant solutions are more reactive than proactive.** The most successful PCI compliance programs include additional tools and services, beyond access to the Self Assessment Questionnaire (SAQ) and Vulnerability Scanning, to help merchants meet specific PCI DSS requirements. The survey data show that acquirers with low compliance achievement rates are more likely to offer breach insurance as a band-aid for poor security controls rather than encouraging layered defenses using security-enhancing tools such as firewalls or end-to-end encryption solutions.

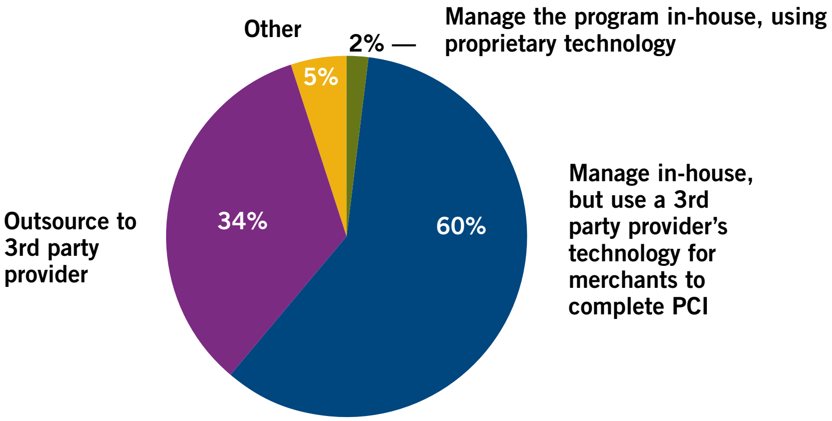
- **They monitor their program less frequently.** Only 20% of those acquirers with a PCI compliance rate under 10% monitor their program on a frequent (daily or weekly) basis, as opposed to 50% of those with compliance rates above 40%. In addition, those with lower compliance rates are much less likely to track merchant attrition. Acquirers who regularly monitor program results, including merchant attrition, remain aware of which merchants need the most assistance and can proactively reach out to keep them engaged in the compliance process.

- **They don't believe their PCI program reduces merchant breaches—and they're right.** Contrary to their successful counterparts, acquirers with low compliance rates are more likely to believe that their PCI program brings no value to their organization, nor to the merchants they serve. In fact, 80% of acquirers with a compliance rate of less than 10% say they don't think their merchants see any value in their program (as opposed to 43% of their counterparts).

As outlined in the previous key finding, acquirers with lower merchant compliance rates feel they have less organizational support for their PCI compliance program. Consequently, they typically have access to fewer internal resources for increasing their program-related activity. In these cases, enlisting a third party to bring in new ideas and proof points on the value of a successful program can produce positive results and momentum.

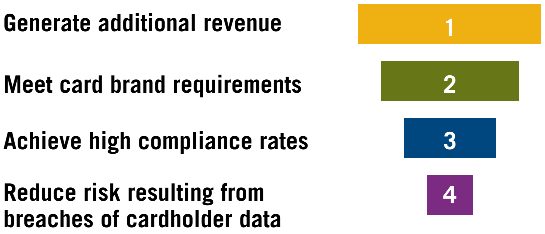
Detailed Findings and Commentary:

1. Who manages your company's PCI compliance program?



The continued trend in PCI compliance program management is to outsource all or a portion of related responsibilities to a third party. Banks and ISOs are most likely to outsource their PCI compliance programs in their entirety.

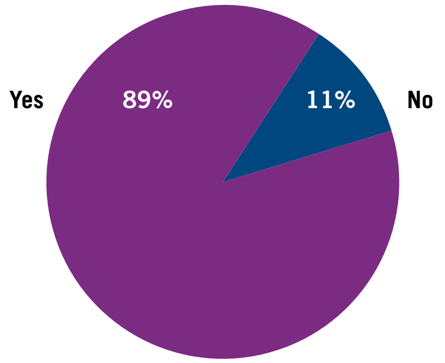
2. Please rank the goals for your company's PCI compliance program (1 is most important).



Responses to this year's survey reflect a notable change in PCI compliance program goals, namely, placing high priority on revenue generation and lower priority on risk reduction. This is a complete reversal from last year's data, providing an important glimpse into the motivators surrounding Level 4 merchant PCI compliance.

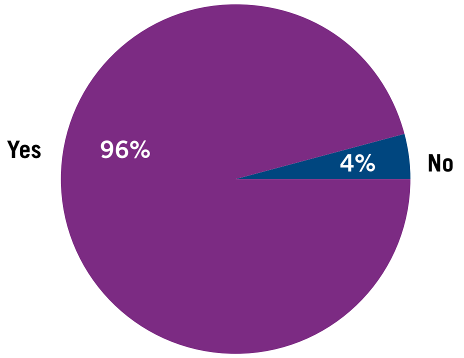
While not all respondents ranked revenue generation as their primary goal, those who do want to generate revenue from the program will need to deliver value-generating solutions to their merchants.

3. Does your current merchant agreement require merchants to be PCI compliant?



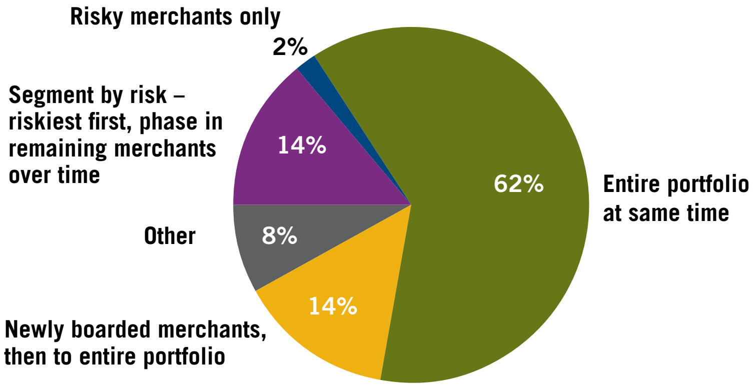
Overall, the percentage of acquirers whose merchant agreements require compliance with the PCI DSS was identical to that of the inaugural survey (89%). Acquirers who do not stipulate PCI compliance within their merchant agreements may not be able to pass down fines in the event of a merchant breach, even if their answer to question 4 below is “yes.”

4. Does your current merchant agreement allow you to pass PCI fines down to the merchant?



While 89% of respondents stipulate PCI compliance within their merchant agreements, nearly all (96%) specify that they will pass along PCI-related fines to the merchant. ISOs, who are less likely to require compliance, are also less likely to pass along fines. By contrast, 100% of bank respondents (as well as organizations with portfolios containing more than 10,000 Level 4 merchants) indicated that their agreements allow them to pass down PCI fines.

5. How did you roll out your PCI compliance program?



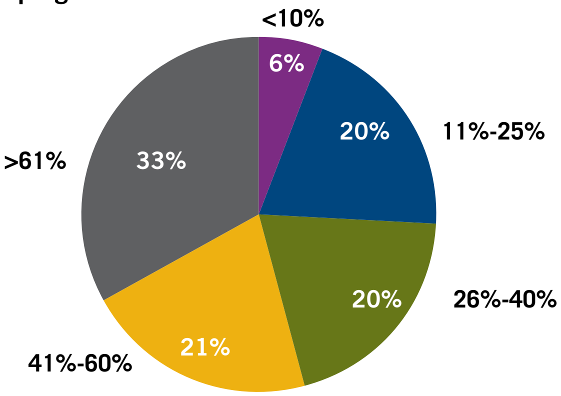
This year's responses show that acquirers still favor a singular PCI program rollout to their entire portfolio (62%), while only 16% are identifying initial program candidates based upon risk. From a portfolio-size standpoint, 29% of acquirers with portfolios of more than 50,000 merchants segmented by risk, while only 6% of those with less than 1,000 merchants did so.

RESPONDENTS' COMMENTS

"We rolled out [our PCI program] to our existing portfolio first, then enrolled new merchants monthly."

The larger the portfolio, the greater the need to segment PCI program activities by risk. This involves evaluating each merchant for specific risk indicators and assigning a corresponding priority to the account. The merchant category code (MCC) is a helpful tool for assessing risk; merchants categorized within hospitality, retail chains, restaurants and universities are especially risky.

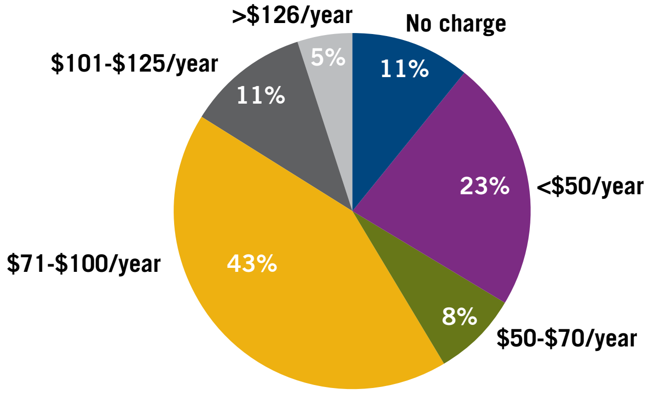
6. What is the current PCI compliance achievement rate for your PCI compliance program?



Overall, the acquirer-reported PCI compliance achievement rates remained relatively similar to last year's numbers within the five categories. There were no banks with less than a 10% achievement rate and 35% of banks reported a >61% achievement rate (representing a 22% category increase over last year).

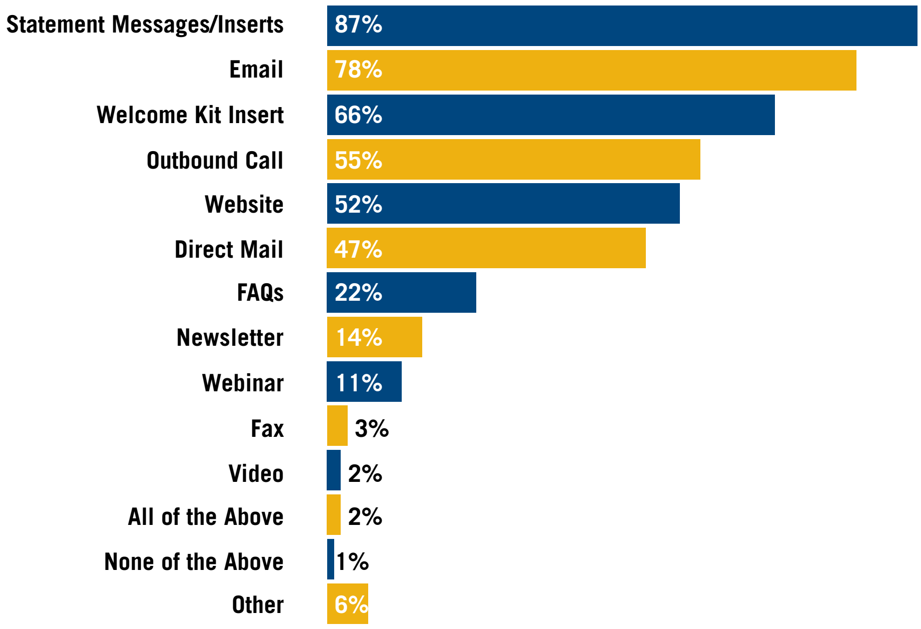
Organizations with smaller portfolios (10,000 or fewer Level 4 merchants) reported higher compliance achievement rates than acquirers with larger-sized portfolios. The survey data show that more than half (53%) of the organizations with the smallest (i.e., <1K) portfolios fully outsource their PCI compliance programs to a third party and 44% have in-house programs but use third-party technology.

7. How much do you charge merchants to participate in your PCI program?



As discussed in the Key Findings section, this is an area where acquirers' strategies differ, with some charging less for their PCI compliance program and some charging more. While last year there was a 50/50 split in those charging $70 or less per year and those charging $71 or more, this year the majority (54%) charge merchants between $71 and $125 annually.

8. What communication channels do you use to educate and notify merchants about PCI and your program? Choose all that apply.



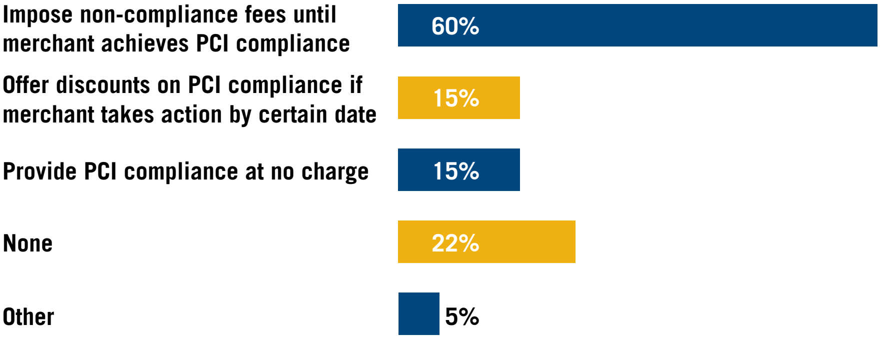
RESPONDENTS' COMMENTS

"[A primary goal for us is] educating the merchant."

Acquirers continue to employ multiple communication channels to engage Level 4 merchants in the PCI compliance process. Last year, the top three channels utilized were statement messages/inserts, email and direct mail. This year, the top two channels are still statement messages/inserts and email; however, the third most utilized channel is welcome kit inserts. More than half of respondents also utilize website messaging and outbound calling to reach out to merchants.

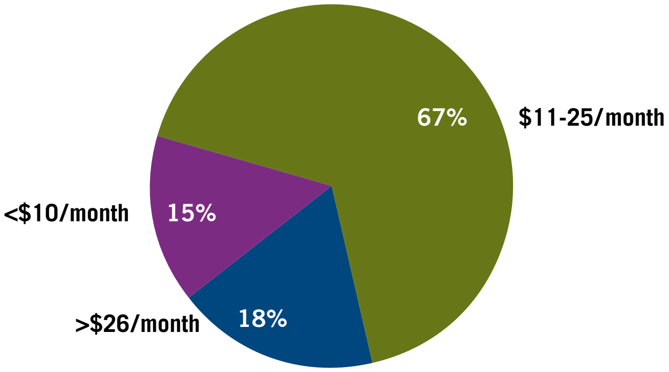
When asked how many times in a year they utilize a communication channel to engage and drive action from merchants in their PCI program, 43% of acquirers said they reach out 2-3 times and 44% said they utilize a communication channel four or more times annually. As discovered in last year's benchmark survey, acquirers need more "touch points" with merchants to see improved PCI compliance rates.

9. Which techniques do you employ to get merchants to take action? Check all that apply.



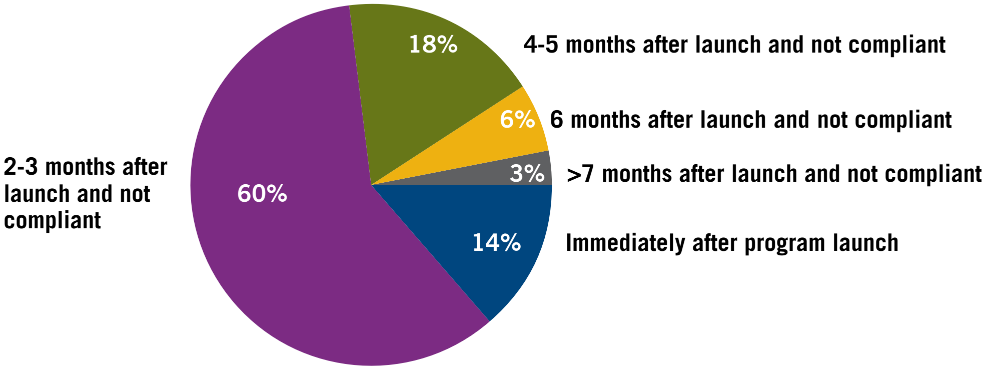
The preferred method for driving merchants toward PCI compliance continues to be non-compliance fees. Use of the "dangling carrot" technique—PCI program discounts in exchange for compliance—has declined since last year. While overall, 22% of this year's respondents admit they don't employ special techniques to increase merchant compliance, only 3% of respondents with the highest compliance rates say they use no techniques.

10. What do you charge merchants for non-compliance fees?



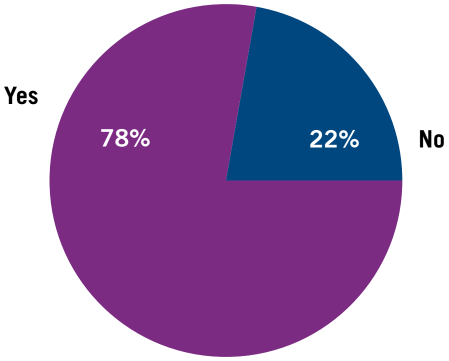
Overall, acquirers are getting more aggressive with non-compliance fees. The percentage of those charging $26 or more per month tripled since last year's survey, and declines in the other two fee brackets support this upward trend.

11. When do you start to impose non-compliance fees?



Not only are non-compliance fees increasing overall, they are also being imposed earlier. Last year, 22% of respondents said they were waiting six months or more to impose non-compliance fees, while this year that number is only 9%.

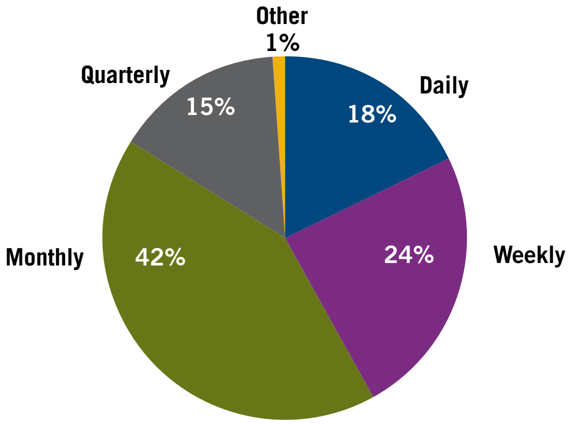
12. Have you found that imposing non-compliance fees has resulted in more merchants achieving PCI compliance?



The majority of acquirers (60%) say they are imposing non-compliance fees as a technique to get merchants to take action with regard to PCI compliance, and 78% of those who charge fees believe the tactic is working.

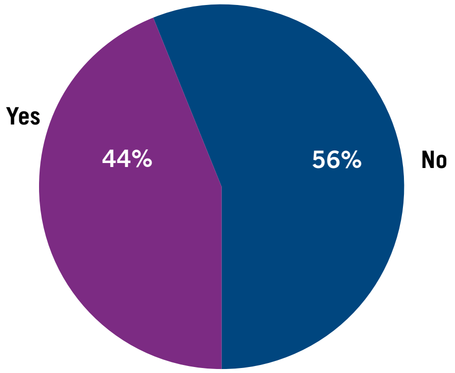
The aforementioned upward trend in monthly fee amount indicates that acquirers believe higher fees will better grab merchants' attention. This belief may be validated by acquirers with the highest compliance rates: 32% are charging more than $25 per month in non-compliance fees while none of those with the lowest compliance rates are doing so. However, given that the majority of the survey's respondents indicate a shift in PCI program goals, it's also possible that non-compliance fees are being used for revenue generation.

13. How often do you monitor the results of your PCI compliance program?



Overall, 42% of respondents say they monitor their PCI compliance program either on a daily or weekly basis, while an additional 42% monitor monthly. Fifty-six percent of acquirers with the highest compliance rates report monitoring daily or weekly, while only 20% of those with the lowest compliance rates do so.

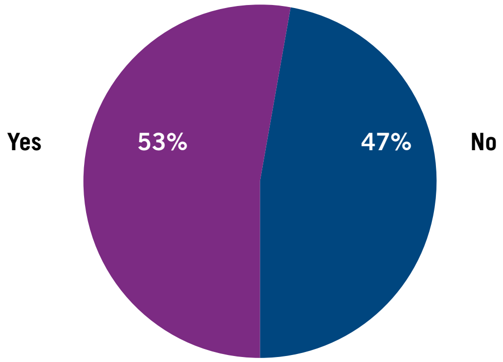
14. Do you offer any additional tools or services, beyond access to the Self Assessment Questionnaire and Vulnerability Scanning, to help merchants meet specific PCI DSS requirements?



Forty-four percent of this year’s respondents say they offer their merchants additional tools or services, down from 52% last year. Acquirers with smaller portfolios (fewer than 5,000 Level 4 merchants) are less likely to offer additional tools than their larger-portfolio counterparts.

Because respondents to last year’s survey included breach insurance in their “other” responses to this question, the service was added among the possible selections for this year’s survey. Interestingly, 60% of respondents indicated that they offer breach insurance to their merchants.

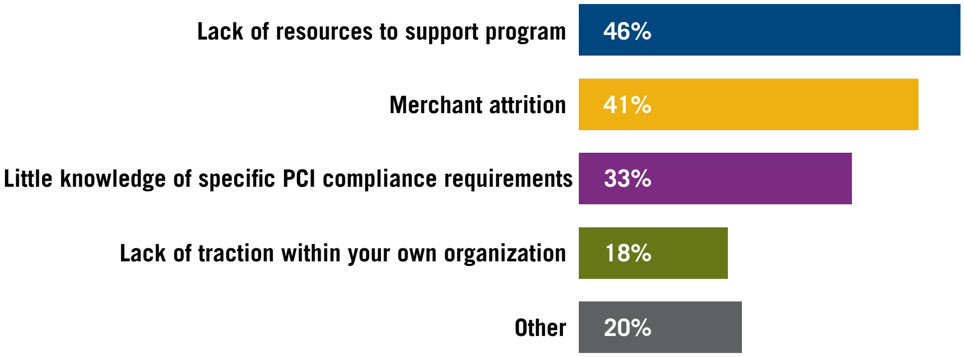
15. Are you currently offering or considering offering end-to-end encryption or tokenization technologies to help your merchants reduce their PCI scope?



Encryption and tokenization are effective technologies for enhancing data security and reducing the card data environment scope. 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. Slightly over half (53%) of acquirers say they are currently offering, or considering offering, these solutions.

More than two-thirds of respondents to the Fourth Annual Survey of Level 4 Merchants have not implemented, and are not yet considering, encryption and tokenization technologies to better secure their business. Acquirers should begin educating their merchants regarding these technologies, so that they are able to make informed decisions as the PCI SSC updates its list of validated encryption solutions.

16. What challenges have you faced in implementing/running your PCI compliance program? Choose all that apply.



Lack of resources remains a primary challenge for acquirers' PCI programs. Sixty percent of acquirers reporting a PCI compliance rate of less than 10% feel their PCI program lacks traction within their own organization, while only 6% of acquirers with the highest PCI compliance rates report the same issue. Similarly, 60% of the "<10%" acquirers also say that they are experiencing a "lack of resources to support" their program. While this is a more commonly reported issue across the achievement-rate brackets, a greater percentage of those with the lowest rates cite it as a concern.

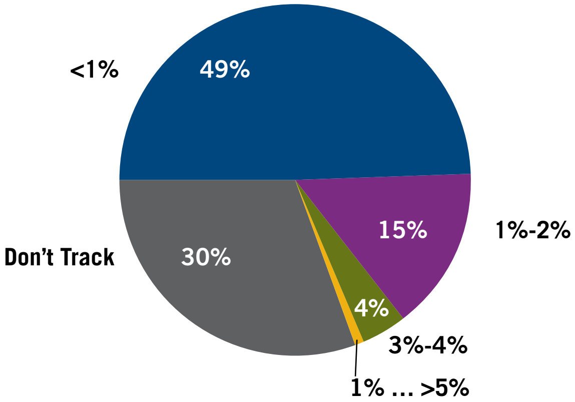
Here are some of the other common barriers acquirers are experiencing in the Level 4 merchant PCI compliance process:

RESPONDENTS' COMMENTS

"You can lead a horse to water but you can't make it drink."

- Overall merchant apathy and lack of response,
- Getting compliant merchants past the annual validation hurdle,
- The technical language within the Self Assessment Questionnaire, and
- Merchants' budgetary constraints and/or skepticism regarding associated costs.

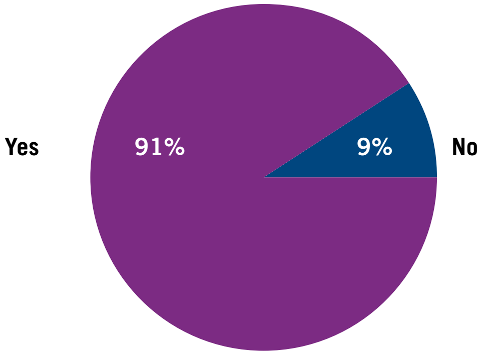
17. What percentage of merchants has left your portfolio on a monthly basis as a result of your PCI compliance program?



Nearly half (49%) of acquirers say that they lose less than 1% of their merchants (on a monthly basis) specifically because of their PCI compliance program. This represents an encouraging 12% increase over last year.

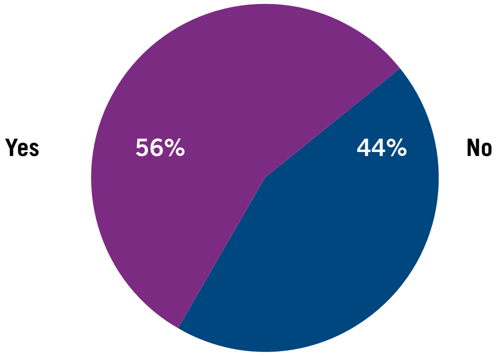
The percentage of acquirers not tracking merchant attrition has remained virtually unchanged, with those reporting the lowest compliance rates continuing to be the least likely to track attrition. What isn't measured can't be improved; therefore, it is important that acquirers track metrics that show the impact of their merchant compliance efforts so they can modify their program as appropriate.

18. Do you work with your merchants to ensure that their third-party service provider(s), gateways, etc., are PCI compliant?



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. Ninety-one percent of respondents indicate that they are helping their merchants connect with reputable third-party service providers, representing a 5% increase from last year's survey.

19. Do you think your merchants value your PCI compliance program?

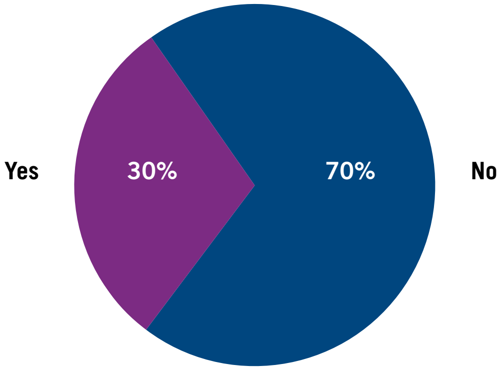


As highlighted in the Key Findings section, there is a strong correlation between acquirers' perception of how merchants view their PCI compliance program and the level of organizational support these acquirers enjoy. In addition, acquirers with compliance rates above 25% are much more likely to believe their merchants value their PCI compliance program.

RESPONDENTS' COMMENTS

"Merchants couldn't care less about PCI, and see it as 'just another fee to take money from' them..."

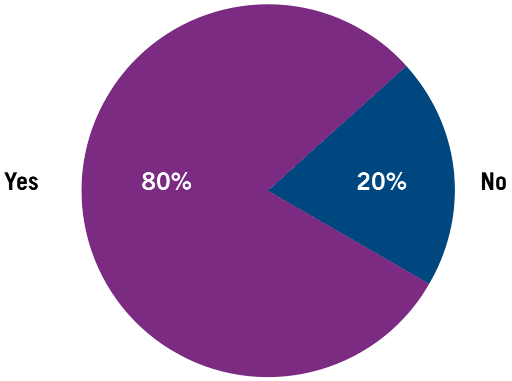
20. Have any of your merchants experienced a data breach in the last 12 months?



Only 2% of Level 4 merchants responding to the Fourth Annual Survey of Level 4 Merchants said they had experienced a data breach in the past year; however, acquirers responding to this survey indicate that small merchant breaches are much more prevalent.

Overall, 30% of acquirers said they had at least one merchant breach in the last 12 months. More than half (52%) of processors indicated that one or more of their merchants had suffered a breach, and a whopping 77% of acquirers with portfolios containing more than 50,000 merchants had at least one breach incident. PCI compliance rates continue to correlate to breach risk; 60% of those with compliance rates under 10% reported having a merchant breach while only 21% of those with compliance rates higher than 60% had experienced a breach incident in the last year.

21. Do you believe that your PCI compliance program has been beneficial in reducing small merchant breaches?



Eighty percent of this year's respondents believe their PCI compliance program helps reduce breaches within their small merchant portfolios—a 10% increase over last year's response. Understandably, 40% of acquirers with the lowest compliance rates don't think their PCI compliance program helps reduce small merchant breaches. As discussed in question 20 above, these acquirers are also more likely to have had a merchant experience a breach in the last year.

Acquirer Recommendations:

Acquirers of all types and with all sizes of portfolios share a common desire to productively serve their merchants' needs. No acquirer wants to lose a merchant to a business-ending data breach, yet ongoing merchant apathy and lack of internal traction can reduce the resolve of staff members who are tasked with managing the organization's PCI compliance program.

Now is not the time to maintain the status quo, however. Emerging payment technologies and new players in the payments space mean that Level 4 merchants have more choices in service providers—and they have a greater need for security-related education and support. Today, merchant acquirers have both an opportunity and a challenge to proactively serve small merchants as a trusted business enabler.

The following recommendations are designed to help acquirers increase Level 4 merchant PCI compliance while growing in their role as a vital merchant partner.

1. Educate merchants early and often.
The best way to motivate merchants to take action is to maintain a consistent message and communicate it frequently through multiple channels, such as direct mail, outbound calls, your organization's website, etc. This tactic ensures that the PCI compliance message is being heard and retained. In addition to creating sufficient awareness, repeating a strong and consistent message builds merchants' trust that you can provide proper guidance.

Merchant trust begins with the sales process, so it's important to provide your sales team with the necessary talking points to ensure PCI compliance is mentioned during the selling process and then reinforced upon boarding. Pay special attention to the message itself to successfully communicate the contribution the PCI DSS makes toward helping the merchant protect their customers and their business.

PCI compliance messages should appear throughout and beyond the merchant onboarding process. Make it your goal to establish clear expectations with all merchants and be sure to enroll high-risk merchants (at a minimum) into your PCI program as soon as they are boarded. When possible, balance electronic and paper-based communications with phone calls and face-to-face conversations.

2. Pursue top-level organizational support for your PCI compliance program.
As discussed in the Key Findings section, achieving internal traction for your PCI program initiatives is paramount to the program's—and your merchants'—success. Organizational backing helps make PCI compliance-related communications a part of your corporate culture, so that all areas of merchant interaction reinforce the relationship between payment transaction security and the overall health of the merchant's business.

When acquirer organizations fully support their Level 4 merchants' PCI compliance process, loyalty builds and more merchants take positive action. Full support doesn't have to entail a large investment of time and resources internally; a reputable third party can serve as a partner to guide each merchant successfully through the process.

Recommendations include taking a risk-and-reward-based approach to senior-level communications and balancing competitive concerns with the benefits of more effective merchant dialogue. Demonstrate how your PCI program impacts merchant loyalty and compliance, measuring key indicators such as merchant attrition and sentiment. Then, as merchants' confidence builds, their compliance rates go up and the number of breach instances decline, organizational leaders will take note and continue their endorsement.

3. Incorporate solutions that bring your merchants value.
Today's small merchant has an increasingly broad array of payment processing choices and tends to migrate toward those that offer the greatest degree of simplicity. In some cases, the solution providers (notably, payment aggregators) absorb risk and don't require merchant compliance with the PCI DSS. Traditional acquirers will need to provide sufficient value to substantiate their PCI-related costs and fees.

The following are suggested ways your organization can bring additional value to your Level 4 merchants:

- **Position your PCI program as a value-added service.** Many acquirers continue to face negative merchant perceptions toward PCI compliance. A robust PCI program brings merchants value through continuous communications and support, helping them successfully meet and maintain compliance requirements, and at the same time understand the important relationship between PCI compliance and a strong security posture.

- **Offer strong support, and technology that simplifies the process, to help merchants overcome any barriers to compliance.** The biggest barrier to Level 4 merchants completing the PCI compliance process is lack of understanding.* Merchants need ongoing education and individualized support services that will help them step through the process. Security services that reduce merchants' scope of compliance, assist them in meeting specific PCI DSS controls and simplify their validation processes also present value.

- **Incorporate breach insurance as a safety net, not as a replacement for PCI compliance.** A surprising finding from this year's study was that 100% of acquirers with the lowest compliance rates are offering breach protection to their merchants. This communicates a lack of confidence that merchants can effectively secure their payment transactions. Breach insurance in and of itself is not a bad thing to have as a safety net; however, PCI compliance should come first.

*Source: A Tale of Two Merchants: The Fourth Annual Survey of Level 4 Merchant PCI Compliance Trends.

4. Deepen your engagement with PCI and your merchants will follow.
A close examination of your merchant communications will reveal what your organization values, and these will be the messages passed along to the merchant. As with any business partnership, your relationship with your merchants will flourish when you communicate shared values. Your organization values cost-effective business operations, because they return a higher profit—and the same holds true for the Level 4 merchant.

Helping the merchant understand that their livelihood depends on secure payment transactions comes from bolstering your organization's internal understanding of payment security. One-third of acquirers responding to this year's survey (a slight increase over last year's 31%) say that their own lack of PCI knowledge challenges their PCI program's effectiveness. Knowledge barriers must be removed in order to remove those same barriers for the merchant.

Many acquirers have found that promoting a general understanding of data security best practices begets merchant action toward PCI compliance. When action steps are presented in a way that's easy to emulate, both the acquirer and the merchant benefit—the merchant's business is protected from breach and the acquirer retains a happy customer.

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 Acquirers' Committee:

MAC is an organization of Bankcard professionals involved in the risk management side of Card Processing. The organization has members from banks, ISOs, card associations and others related to the risk management side of the industry. MAC is dedicated to providing universal risk management solutions through ongoing communication and cooperation among acquirers and card associations. For more information visit www.macmember.org or email info@macmember.org.