THE IMPACTS OF BREACHES

DR. BRANDEN R. WILLIAMS & MAC

A SURVEY OF MAC MEMBERS ON THE REALITIES OF DATA BREACHES

info@brandenwilliams.com | www.brandenwilliams.com

CONTENTS

INTRODUCTION AND METHODOLOGY 4

ASSUMPTIONS AND LIMITATIONS 4

KEY FINDINGS 6

RECOMMENDATIONS 12

CONTACT 13

EXECUTIVE SUMMARY

Major data breaches in the merchant community are costly for organizations. However, the scope of the problem across the merchant community may not be as extensive as common knowledge suggests. That's one of the conclusions of an analysis of a survey of Merchant Acquirers' Committee (MAC) membership jointly sponsored by MAC and BrandenWilliams.com in the fourth quarter of 2014. This whitepaper presents the results of this survey analysis.

The survey is somewhat unique in the industry as respondents cut across the Payment Card Industry Data Security Standard (PCI DSS) compliance ecosystem, rather than focusing on the customers of a single vendor or payment brand. The data collected is limited to members of MAC who are primarily US-based. Analysis of the findings also reveals that PCI compliance rates remain lower than advertised, suggesting that compliance systems currently in use to manage large merchant populations may be inadequate to promote higher compliance rates. The results also indicate that consumers typically do not change their spending habits after breaches.

Merchants remain responsible for their own security in the PCI ecosystem and compliance with all appropriate standards. Firms that choose to accept payment card data in exchange for goods and services must prepare for the inevitable attack and the risk of compromise. The relatively low number of breaches and the small amount of fines assessed (as revealed in this study) provides little incentive for acquirers and processors to quell breaches through proactive measures. Acquirers should take a more active role of the breach problem by investing in technology that protects merchants while they process payment data. Merchants may perceive this value-added service as a reason to continue their current processing relationship, and it could offer acquirers a competitive advantage.

INTRODUCTION AND METHODOLOGY

In September and October of 2014, Branden Williams conducted a survey in partnership with the Merchant Acquirers' Committee (MAC) to enhance the understanding of data breaches among merchants. One of the primary goals was to build upon the many existing studies that examine the costs and scope of data breaches while removing some of the bias inherent in those studies[1]. For example, a forensic vendor's survey is limited to the customers in their database, and a payment brand's survey is limited to their customers. By contrast, this study cuts across vendor and payment brand customers by surveying a portion of MAC members. The inherent bias in this survey is that it only includes U.S. entities that are members of MAC. This is consistent with the intended scope of this survey.

The MAC community includes acquirers/merchant banks, processors, independent sales organizations (ISOs), and others. MAC membership exceeds 500 firms. Approximately 20% of MAC members participated in the survey (although not all survey responses could be used in the analysis due to incomplete responses).

ASSUMPTIONS AND LIMITATIONS

This research attempted to remove as much bias as possible to obtain results that could translate to the larger population of MAC members. There are two major limiting factors to this research. The first is the lack of complete responses. The survey instrument used in this research asked detailed questions about breaches that may have extended beyond many members visibility into their current situation. This by itself may indicate how well MAC members are managing risk. The second is the lack of normal distributions in the data. The analysis used algorithms that have built-in robustness against non-normal data.

[1] Most of these studies are biased toward the customer groups in the surveying company's datasets.

Finally, a word about correlation and causation as several variables in the analysis indicate correlation. Correlation indicates that the data in the specific groups move together in the same direction at the same time. Meaning, an action that causes an increase in one group would also show up as an increase in another group. Correlation does not indicate causation, as movement in one variable does not necessarily cause movement in another—even when they move together.

KEY FINDINGS

An analysis of the survey results reveals eight conclusions of interest to ISOs, acquirers, processors, and other merchant service providers. These key findings clarify the current state of Payment Card Industry Data Security Standard (PCI DSS) compliance in the U.S. and offer insights into the scope and consequences of data breaches in merchant communities. While this study addresses all four merchant levels, several of the key findings are particularly relevant to Level 3 and 4 merchant communities—many of which are small to medium-sized businesses.

Compliance rates by level are lower than many entities suggest: Survey results show that PCI compliance rates remain below 70% across all merchant levels (see Figure 1). This indicates that while compliance efforts are underway, acquirers and other entities have quite a bit of work to do to boost compliance rates. It may also indicate that current incentive structures do not promote high compliance rates among acquirers.

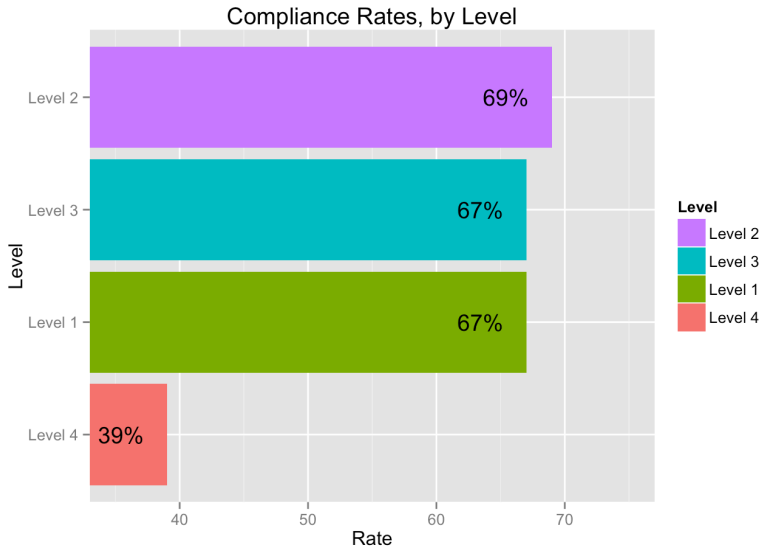

Figure 1. Compliance Rates by Merchant Level

Level 1 and Level 2 compliance program success indicates strong correlation: Analysis of the data indicates a strong positive correlation between Level 1 and 2 compliance rates in the respondents. Given the initial focus of compliance on Level 1 merchants first, then a transition to Level 2 merchants, the data suggests that acquirers manage those programs very closely and achieve similar compliance rates between the two groups. This intuitively makes sense as those groups represent the vast majority of processed transactions.

Level 1 and Level 3 breaches are correlated, potentially due to e-commerce: Analysis of the survey responses also indicates a strong positive correlation between Level 1 breaches and Level 3 breaches. The common factor between the two groups is the e-commerce acceptance channel, which could suggest that these kinds of breaches represent a significant portion of the respondents. None of the respondents reported any Level 2 merchant breaches in the prior year; however, we are aware that a Level 2 breach was reported after the survey closed. Therefore, it is not possible to conclude if there could or would be correlation due to e-commerce activity in that level.

Repeat breaches and Level 4 breaches are correlated: Perhaps one of the more telling correlations is between repeat breaches and Level 4 breaches. The data indicates that acquirers who see high levels of Level 4 merchant breaches may be the most likely to see repeat breaches within 12 months of the initial breach. The survey did not allow the respondent to select the level in which those repeat breaches occurred, but the consensus is that the repeat breaches occurred in the Level 4 population.

There is no one level more likely to be breached than another: An analysis of variance across the three groups who reported data breaches (levels 1, 3, and 4) reveals no statistically significant difference between those breaches by level, regardless of whether or not Level 2 breaches are included in the analysis. According to this data, there is no statistical difference that suggests one group is more likely to be breached than another.

A larger merchant population is directly correlated with lower compliance rates: The data shows that as the number of merchants in a compliance program ("merchant counts") increases, overall compliance rates in that program decrease. This suggests that the systems currently in use to manage large merchant populations may be inadequate to promote higher compliance rates. This conclusion makes sense for the following reasons:

- Intuitively, a larger number of business relationships is more difficult to manage than a smaller number of business relationships.
- The number of merchants in a given compliance program tends to be high in the Level 4 community (businesses with the overall smallest number of transactions, but a larger number of different merchants). Figure 1 shows that Level 4 merchants have the lowest overall compliance rates in the study (39%). Hence, it is not surprising that the Level 4 merchants pull the compliance trend downward as the number of merchants increases.

The survey also segmented the data by type of compliance program:

- In-house with in-house technology
- In-house with a third-party portal
- Outsources to a third party
- Other (combination of outsourcing and in-house)

Figure 2 shows how the compliance rate decreases and the merchant count increases for each of the four types of compliance programs. In the context of the "Other" category, respondents indicated they managed this with some kind of combination of the other three categories. Figure 3 shows that this trend is also true within three of the four merchant levels.

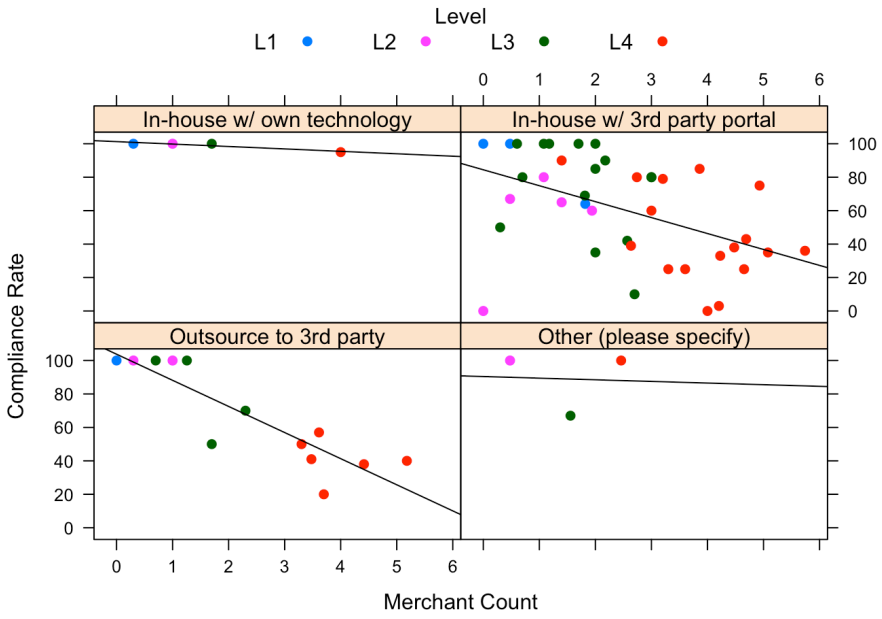

Figure 2. Compliance Rates Decrease as Merchant Counts Increase

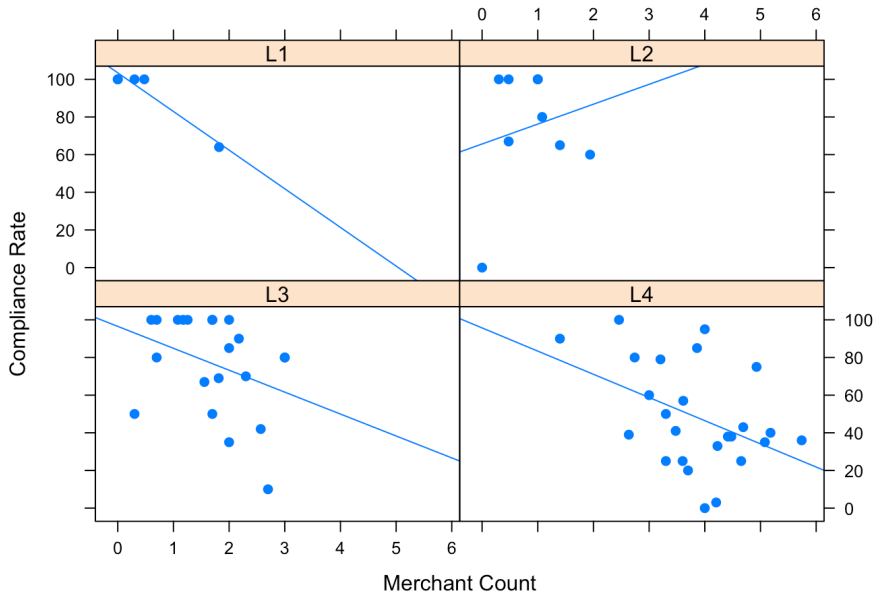

Figure 3. Compliance Rates by Merchant Level & Group Size

Breaches and fines are relatively small and localized: One of the key goals of this survey was to understand the severity of the breach problem for smaller merchants. According to the results in this survey, the financial impacts of the breach problem do not appear to be as severe as perceived or as advertised in the media and other surveys. Level 1 breaches make headlines and significantly impact those companies. However, only 119 of the 1,144,681 merchants included in the results were associated with a breach, with 5 of them reporting more than one breach in the previous 12 months. This equates to 0.01% of the total merchant count.

Of the 119 total breaches reported in the study, only two respondents described fines assessed. Using the data associated with just those two respondents, the average breach cost was $18,500 per incident. *Please note this information is for illustrative purposes only. Under no circumstances does Branden Williams or MAC recommend use of this figure for any risk-based calculation.*

Post-breach transaction levels indicate that consumers do not significantly alter spending habits after breaches: The survey also assessed whether transaction volume changes after a breach. The majority of respondents (69%) reported unknown changes in transaction volumes, while 27% reported no change at all, and only 4% reported a decline (see Figure 4). Unknown transaction changes could be related to a lack of data or a specific desire to track it because it is assumed to remain steady. Common business sense would suggest that if breaches caused a massive decline in transaction volume, acquirers would work to quell this decline through proactive security measures.

Although the large response of unknown changes may impact conclusions, the data suggests that the general public does not change their shopping behaviors at breached merchants over the long term. Given that customers continue to shop and pay with payment cards at breached merchants, there is little motivation to change behavior based on the fear of declining customer sales.

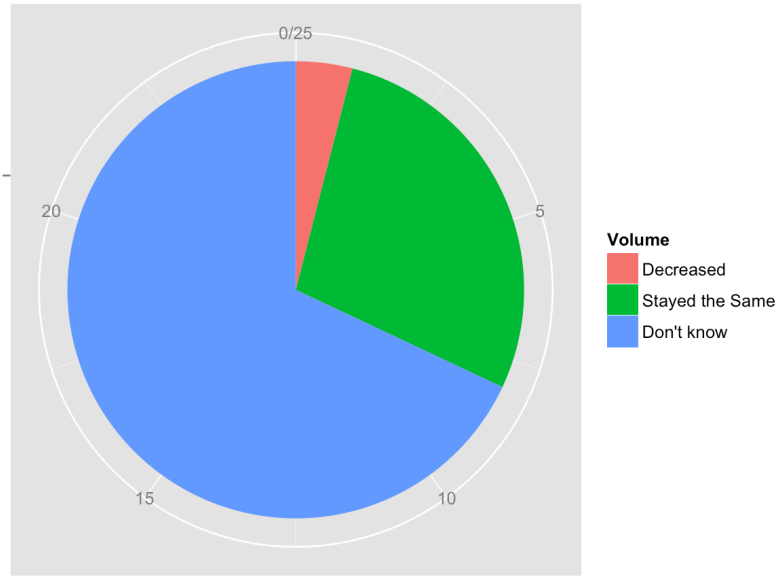

Figure 4. Transaction Volumes after a Breach

RECOMMENDATIONS

Given the relatively low number of breaches and the small amount of fines assessed (as revealed in this study), acquirers and processors have little incentive to quell breaches through proactive measures. These entities can either absorb the losses or pass them along to merchants instead of proactively working to address the issue. It simply is not a big enough business problem for the majority of firms in the ecosystem.

In the case that this changes, firms may consider investing in tools that effectively remove the merchant from the need to address PCI DSS and charge a premium for those tools. Merchants should perceive an actual reduction in breach incidents and little to no risk associated with payment card acceptance. Merchants may perceive this value-added service as a reason to continue their current processing relationship, and it could offer acquirers a competitive advantage.

Major breaches do happen and have been costly for several organizations. However, the scope of the problem across the merchant community may not be as extensive as some believe. Nevertheless, merchants are responsible for their own security in the PCI DSS ecosystem. PCI DSS is complex, and many merchants do not fully understand the inner workings of the standard, how it applies to them, and how to ensure their technology partners are properly securing their data. If an entity chooses to accept payment cards, they must be prepared for a breach to occur or partner with a company who will take the responsibility for handling this data securely.

CONTACT

For more information or to ask additional questions about this survey, please email info@brandenwilliams.com.

ABOUT THE SURVEY SPONSORS

Dr. Branden R. Williams has almost twenty years of experience in technology and information security, as both a consultant and an executive. His specialty is navigating complex landscapes, such as compliance, security, technology, or business, and finding innovative solutions that save companies money while reducing risk and improving performance. You can see information on his three books on PCI Compliance and his other publications at www.brandenwilliams.com.

Merchant Acquirers' Committee (MAC) is an organization of Bankcard professionals involved in the risk management side of Card Processing. MAC members are from Banks, ISOs, Card Associations, and others related to the risk management side of the industry. MAC's mission is to strengthen the payment ecosystem through ongoing education, communication, and cooperation among acquirers, card brands and enforcement agencies. For more information, please visit www.macmember.org.