CONSUMER ATTITUDES TOWARD BREACHES

DR. BRANDEN R. WILLIAMS & MAC

HOW CONSUMERS REACT TO RETAIL BREACHES

info@brandenwilliams.com | www.brandenwilliams.com

CONTENTS

EXECUTIVE SUMMARY

Managers of retail firms fear data breaches, yet breaches happen with a high enough frequency that suggests apathy or a lack of information security savvy to prevent them. Vendors and research firms alike drop sound bites of doom and gloom with respect to consumer behavior, but many firms who suffer breaches don't seem to fail overnight. Consumers who may be vocal about their displeasure with companies that suffer a breach do not seem to change their buying behavior at those breached merchants. That's one of the conclusions of an analysis of a survey sponsored by the Merchant Acquirers' Committee (MAC) in the second half of 2015. This whitepaper presents the results of this survey analysis.

The goal of this research was to understand consumers' attitudes toward breaches. Do consumers really change their buying behavior at breached merchants as some group's suggest? Much research in this area asks questions on the likelihood of a consumer returning to a hypothetical merchant who suffered a breach, which appears to yield misleading results. For this research, survey respondents detailed their spending and shopping habits as well as their awareness of specific public breaches. Not surprisingly, awareness of breaches was limited to two major events—Target Stores and Home Depot. Consumers, for the most part, returned to shop at breached merchants and continued using payment cards to transact business.

Merchants do suffer significantly from breaches, but not at the hands of consumers. Breaches negatively affect cash flow, cash reserves, capital structure, and the careers of executives more than retail sales (1,2). Merchants must boost the security of their payment flow by using technologies such as encryption and tokenization—preferably managed by a processor or acquirer—to reduce the likelihood of a card-related breach.

This report reveals key insights about consumer behavior related to breached merchants, and provides some recommendations for managers of firms who make frequent decisions on breach- and compliance-related initiatives.

INTRODUCTION AND METHODOLOGY

In the second half of 2015, Dr. Branden Williams conducted a survey in partnership with the Merchant Acquirers' Committee (MAC) to understand consumer attitudes toward breaches. Since 2013, a number of major retail establishments have suffered significant payment card breaches. The most recognizable, Target Stores, happened during the 2013 holiday season and caused consumers to react negatively through various forms of media. A prominent research organization published a statistic that suggests payment card breaches directly affect the sales for these merchants. In their research, 28% of all consumers would avoid certain merchants if their data is misused (3). For the companies with publicly traded stock, their quarterly performance filings and additional empirical research suggest otherwise (1).

The goal of this survey instrument was to more directly measure consumer behavior to understand if a breach will cause a consumer to avoid shopping at a particular merchant. Instead of using a Likert-scale to measure the likelihood of a consumer's return to a merchant that suffered a breach, consumers were asked a number of activity-based questions after a breach was made public. In order for a merchant to qualify for inclusion, the firm must have had some kind of public disclosure notice and conducted business on a regional (multi-state) or national level in the United States. Consumers answered questions based on the following breaches presented in random order (name of merchant with date of disclosure):

- Target Stores, Dec 13, 2013
- Neiman Marcus, Jan 14, 2014
- Michael's Stores, Jan 25, 2014
- Sears, Feb 28, 2014
- Sally Beauty Supply, Mar 5, 2014
- Aaron Brothers, Apr 17, 2014
- Goodwill Retail Stores, Jul 14, 2014
- The UPS Store, Aug 20, 2014
- Dairy Queen, Aug 27, 2014
- The Home Depot, Sep 2, 2014
- Albertson's, Sep 29, 2014
- K-Mart, Oct 10, 2014
- Staples, Oct 20, 2014
- Bebe, Dec 5, 2014
- Toys "R" Us, Mar 3, 2015

This survey, conducted through SurveyMonkey, resulted in 1,031 complete responses. In order to qualify, consumers must have the following characteristics: own a credit or debit card, live in the United States, be aged between 18 and 70, and have an income of over $30,000 annually. Consumers were asked about their awareness of a breach at the above merchants and their spending behavior. In order to proceed to the questions around spending behavior, consumers must have shopped at one or more of the breached merchants in the last three years.

For consumers that had shopped within twelve months of any of the breaches, they indicated how quickly they returned to any of the stores (or in the case that they have not, that was indicated as well) who suffered a breach. They then indicated how they paid, and for those that did not return, they responded with a reason why.

From a demographical perspective, the gender breakdown was nearly even at 50% male and female, 40% of the respondents were between 45 and 59, 31% were between 30 and 44, 16% were over 60, and 13% were between 18 and 29. The total household income for every respondent was at least $50,000, with 8% over $200,000.

ASSUMPTIONS AND LIMITATIONS

One major limitation to this research (and suggestion for future research) is that all of the breaches investigated were done on a country-wide scale. All of the affected companies were either large private institutions or public companies, all residing in the United States. This research does not examine consumer attitudes toward breaches of smaller companies for a number of reasons—the largest of which is that most of those breaches are not made public. While these findings may be able to be applied to those smaller types of firms who will have the same pressures around reacting to a breach, consumers may react differently to a small company suffering a breach—either positively or negatively.

This research only attempts to measure consumer behavior related to a breach and does not take into account business-to-business arrangements or non-payment card breaches. For example, the CardSystems Solutions breach from 2005 that lead to Visa and American Express pulling their contracts, forcing the company to sell the business. In addition, non-payment card data such as Personally Identifiable Information or Electronic Health Records (other sensitive consumer data) disclosed in a breach that leads to identity theft may result in differing attitudes and spending patterns, as well as more severe penalties for the breached firm.

KEY FINDINGS

This analysis reveals four conclusions of interest to merchants, acquirers, processors, and other payment service providers. Breaches represent a flash in the history of the firm—usually sparking intense activity in response to the incident, which tapers over time. In many cases, breaches repeat themselves due to a lack of long-term focus on information security. As an example, Target's 2013 breach was the second in eight years with the other happening in 2005. Thus, short-term actions tend to be reactionary with some resulting in strategic direction changes over time.

Awareness of breaches is poor in general, with two notable exceptions: Data breaches happen at such a frequency that the general public may be desensitized to them. Consumers, in general, displayed little awareness of the breaches presented to them. Perhaps this is one of the key indicators of their attitudes toward these breaches. Only Target Stores (81%) and The Home Depot (38%) represented a significant breach awareness. Of the responses, 13% indicated no awareness of any of the data breaches presented.

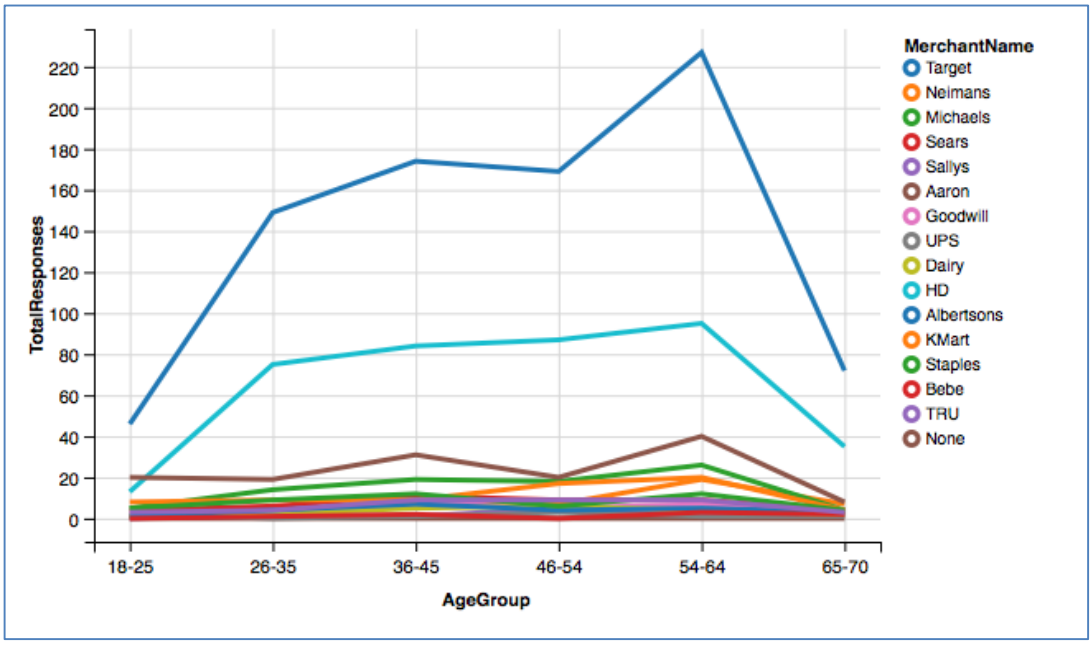

Figure 1. Awareness of breaches by age group.

Perhaps an interesting finding to pull from this group is the awareness in the 54-64 age range group. These respondents appeared to be the most aware group visually, however, there was not any statistically significant variance between the groups (p = 0.547). In fact, no demographical check that we compared (Income, Region, Device survey was completed on, or Gender) had any statistically significant findings that suggest one group was more aware of breaches than another.

In addition, the data indicates that older consumers are more likely to defect because of the breach with nearly three quarters of the defectors being over the age of 46.

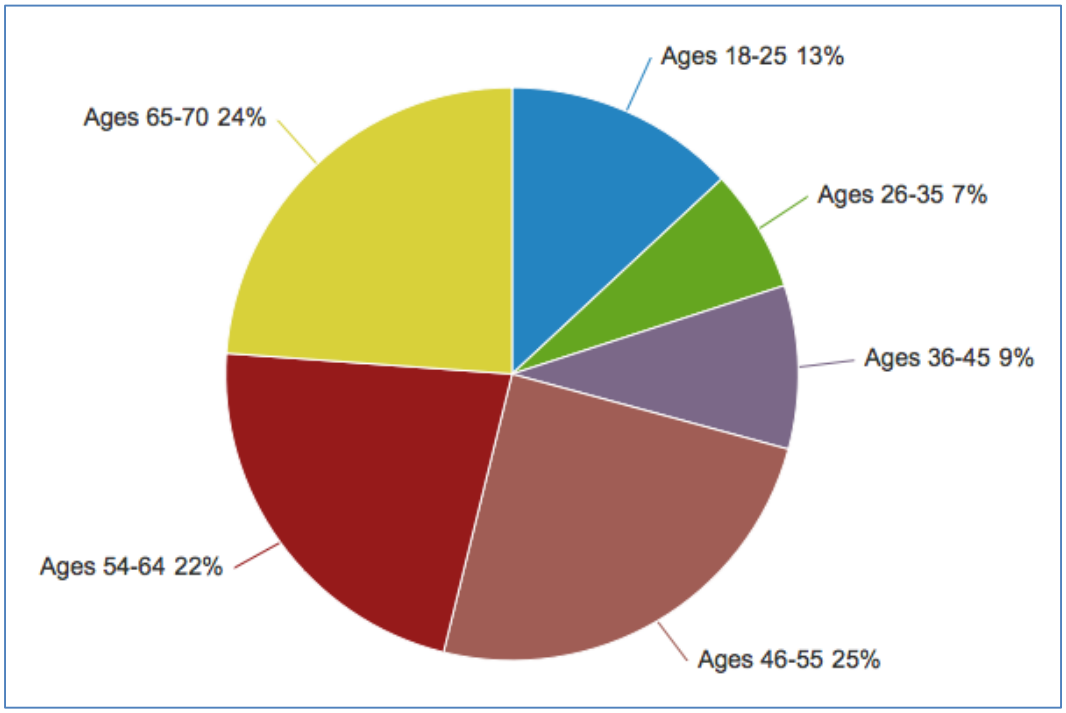

Figure 2. Age distribution of defectors.

Consumers are quick to return to breached merchants: In every single case, the majority of consumers returned to that location nearly three months after the breach. Consumers returning to shop at these locations may not have been aware of the breach, which taken alone is a finding for discussion. They appear to either be unfazed or unaware of breaches in a way that materially changes their shopping behavior. Less than 2% (on average) have not returned since a breach went public.

Based on the means from the responses, shoppers tend to return to shop between three and six months from a breach if they were aware of the breach. No one age group demonstrated more propensity to return faster over another ($p = .475$). With the wide range of merchants included in the breach, the type of goods or services sold matters when determining how quickly consumers will return. Suppliers of necessities such as food or non-durable goods see quicker returns than others ($p < 0.001$).

Figure 3 depicts visual means of the response data. Survey respondents chose either (1) returned within 30 days, (2) returned within 3 months, (3) returned within 6 months, (4) returned after 6 months to present day, or (5) did not return.

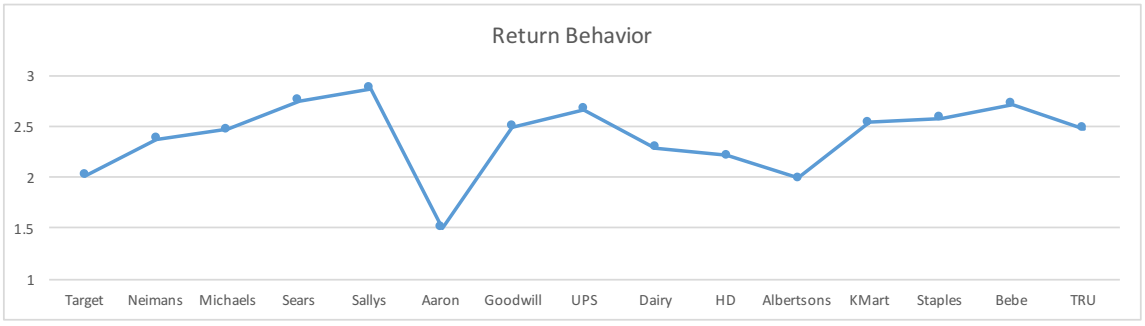

Figure 3. How quickly do people return?

Consumers continue to favor payment cards over cash or check: Even in spite of merchants suffering from a breach involving the payment cards in consumers' wallets, consumers still prefer to use cards over other methods of payment. Fully 78% of respondents (on average) paid with a credit or debit card after said merchant's breach with cash following at a distant second. Respondents over 46 demonstrated a slightly larger preference for cash over other groups.

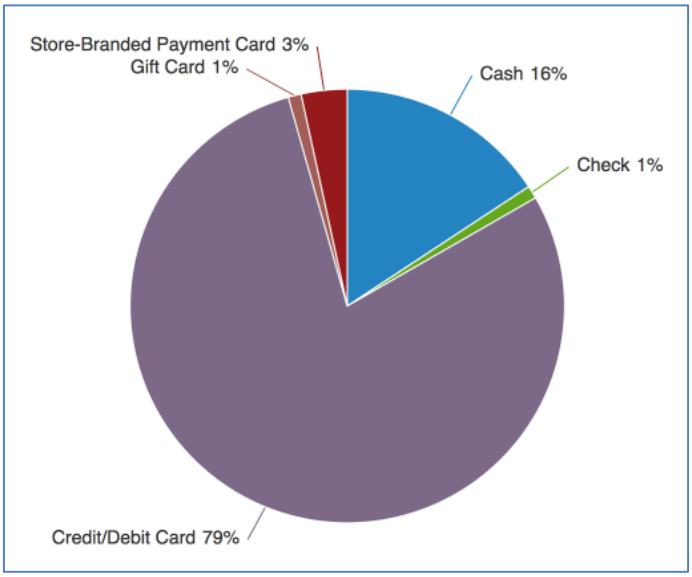

Figure 4. How consumers paid, post breach.

The biggest reason for not returning to the merchant was not related to the breach: When asked why consumers who had shopped at one of the breached merchants in the last three years did not return to the merchant within twelve months of the breach, 70% indicated that they do not regularly shop at the merchant in question. Consumers who stood their ground against compromised merchants were in the minority. Only 4% took their business to a competitor that they perceived to be more secure, with an additional 2% indicating they did not return specifically because of the breach.

What is not captured here is the impact of subscription services such as Amazon Prime to face-to-face merchants. It is unclear whether the growth of services like Prime over the last several years contributed to the irregularity of consumers shopping at the merchants included in the survey.

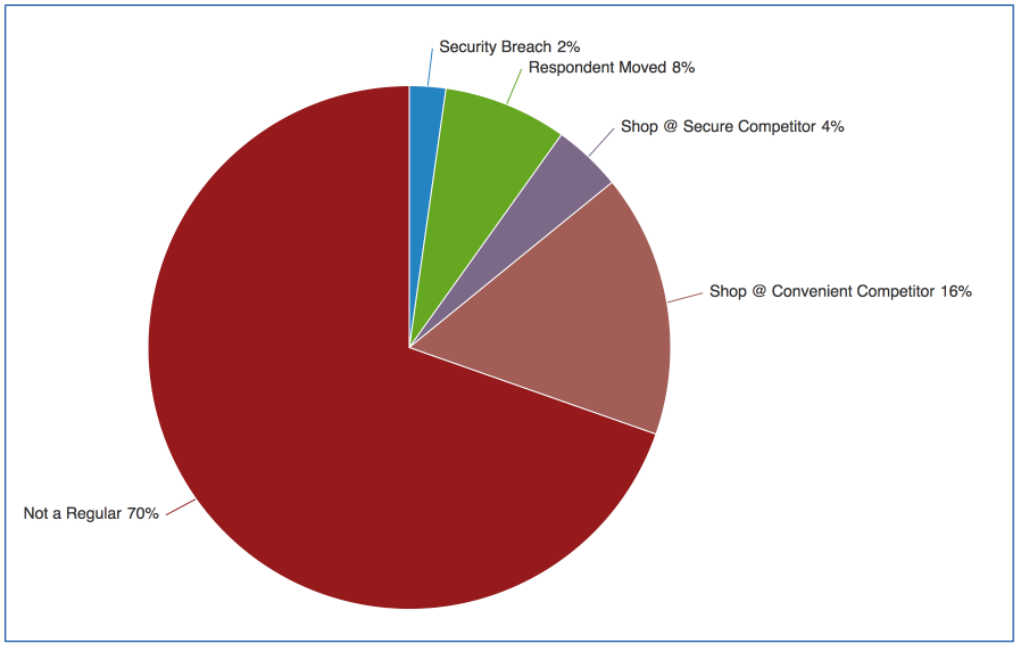

Figure 5. Why consumers didn't return.

RECOMMENDATIONS

This research indicates, for the most part, that consumers do not feel enough harm, or simply do not care enough about payment card breaches to change their spending behavior. Breached merchants are not immune to drops in sales or revenue, but the research indicates that any decline is temporary. Lost revenue will be replaced by new or existing customers unaware of the breach or consumers habitually returning to stores as part of their shopping routine. The rate of return may be dependent on the types of goods sold, *ceteris paribus*. Merchants who sell everyday goods may be more insulated than those whose customer base shops less frequently.

In other words, an information security breach might be the digital equivalent of a natural disaster, such as floods or a hurricane. The event causes a minor interruption in operations with a significant capital outlay to clean up and return to normal operations.

Managers of firms that suffer a breach must be mindful of cash flows after a breach announcement from temporary sales gaps accompanied by a significant uptick in firm spend related to clean-up efforts. Common costs that firms face in the wake of a payment card breach include investigation and forensic services, legal fees, consulting fees, IT and security infrastructure, headcount increases to support new systems, and reserves held for lawsuit settlements (4). Some merchants may see a loss in value through charges to Goodwill, thus reducing the asset side of the balance sheet. In addition, a merchant's processor or acquiring bank may withhold settlement funds to cover costs in the case that the merchant's post-breach solvency is in question.

Risk managers in firms that use payment card data should evaluate the controls they have in place to protect this data. In the case that the data is housed or handled by the merchant directly, steps should be taken to boost the security of the payment flow through technology, such as encryption and tokenization—preferably managed by a processor or acquirer—to reduce the likelihood of a breach. Payment card breaches directly affect shareholder value in a firm through unexpected spending in their wake.

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 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 multiple 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.

Endnotes:

1. Hinz O, Nofer M, Schiereck D, Trillig J. The influence of data theft on the share prices and systematic risk of consumer electronics companies. Inf Manag. 2015 Apr; 52(3):337–47.
2. Smith D. Data breaches sink senior management careers. MHD Supply Chain Solut. Intermedia Group; 2015 Oct; 45(5):64.
3. 2015 Identity Fraud: Protecting Vulnerable Populations. 2015.
4. Layton R, Watters PA. A methodology for estimating the tangible cost of data breaches. J Inf Secur Appl. 2014 Dec; 19(6):321–30.