Ponemon INSTITUTE

The Aftermath of a Data Breach: Consumer Sentiment

Sponsored by Experian® Data Breach Resolution

Independently conducted by Ponemon Institute LLC

Publication Date: April 2014

The Aftermath of a Data Breach: Consumer Sentiment

Ponemon Institute, April 2014

Part 1. Introduction

Data breaches are in the headlines and on the minds of both businesses and consumers. While much of the dialog has been driven by companies that experienced a data breach, this new study sponsored by Experian® Data Breach Resolution explores consumers' sentiments about data breaches. Our goal is to learn the affect data breaches have on consumers' privacy and data security concerns. A similar study was conducted in 2012 and reveals some interesting trends in consumers' perceptions.

As part of the study, we asked consumers who were victims of a data breach questions about their experience. It may not come as a surprise that individuals who have had their personal information lost or stolen increased 100 percent since the 2012 study when only 25 percent of individuals surveyed were victims of a data breach.

For purposes of this research, we define a data breach as the loss or theft of information that can be used to uniquely identify, contact or locate you. This includes, but is not limited to, such information as Social Security number, IP address, driver's license number, credit card numbers and medical records.

A total of 797 individuals were surveyed and approximately 400 of these respondents say they were the victims of a data breach. By far, the primary consequence of a data breach is suffering from stress (76 percent of respondents) followed by having to spend time resolving problems caused by the data breach (39 percent of respondents).

The major themes of this research are as follows:

- Consumers' perceptions about organizations' responsibility to the victims.
- Trends in the experiences of data breach victims.
- The impact of media coverage on consumer sentiment about data breaches.

Following are some of the most salient findings of this research:

What companies should do following a data breach. Most consumers continue to believe that organizations should be obligated to provide identity theft protection (63 percent of respondents), credit monitoring services (58 percent) and such compensation as cash, products or services (67 percent). These findings are similar to the findings in the 2012 study.

Credit card companies and retail stores sent the most notifications. Sixty-two percent of respondents say they received two data breach notifications involving separate incidents. These notifications can be in the form of a letter, telephone call, email or public notice.

Becoming a victim of a data breach increases fears about becoming an identity theft victim. Prior to having their personal information lost or stolen, 24 percent say they were extremely or very concerned about becoming a victim of identity theft. Following the data breach, this concern increased significantly to 45 percent. Forty-eight percent of respondents say their identity is at risk for years or forever.

How important is media coverage of data breaches? The majority of respondents believe it is important for the media to report details about data breaches. Mainly because it requires companies to be more responsive to victims followed by the creation of greater awareness about how the data breach could affect individuals and alerts potential victims to take action to protect their personal information from identity theft.

Part 2. Key findings

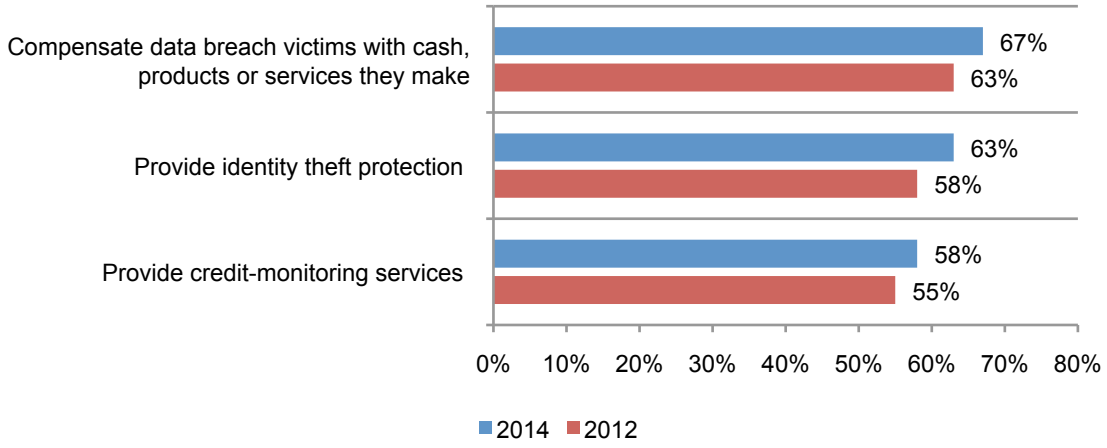
In this section, we provide an analysis of the key results. The complete audited findings are presented in the appendix of this report.

- Consumers' perceptions about organizations' responsibility to the victims
- Trends in the experiences of data breach victims
- The impact of media coverage on consumer sentiment about data breaches

Consumers' perceptions about organizations' responsibility to the victims

What companies should do following a data breach. Most consumers continue to believe that organizations should be obligated to provide identity theft protection (63 percent of respondents), credit monitoring services (58 percent) and such compensation as cash, products or services (67 percent), as shown in Figure 1. These findings are similar to the findings in the 2012 study.

Figure 1. Organization's obligation following a data breach
Strongly agree and agree responses combined

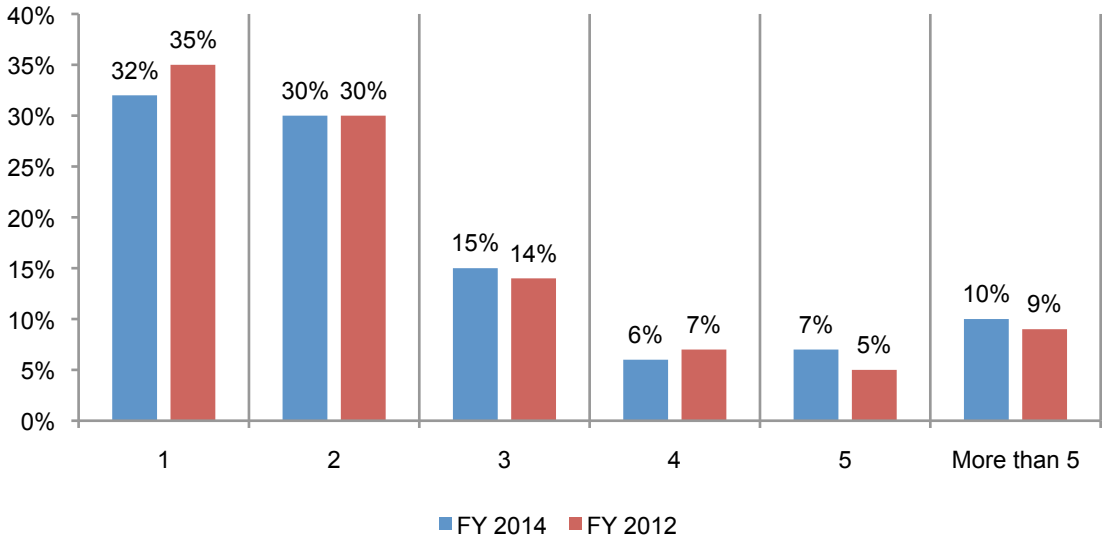


Trends in the experiences of data breach victims

As part of the study, we asked consumers who were victims of a data breach questions about their experience. Fifty percent of respondents in this year's study say they received at least one data breach notification. Only respondents who had a data breach in the past two years participated in this part of the study.

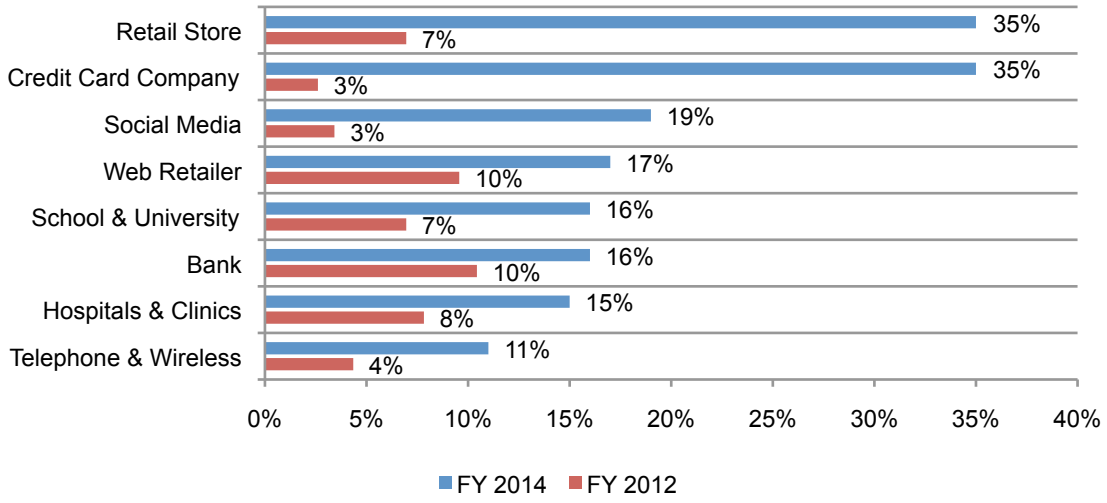
Credit card companies and retail stores sent the most notifications. According to Figure 2, 62 percent of respondents say they received two data breach notifications involving separate incidents. These notifications can be in the form of a letter, telephone call, email or public notice.

Figure 2. Number of data breach notifications received for <u>different incidents</u> in the past 2 years



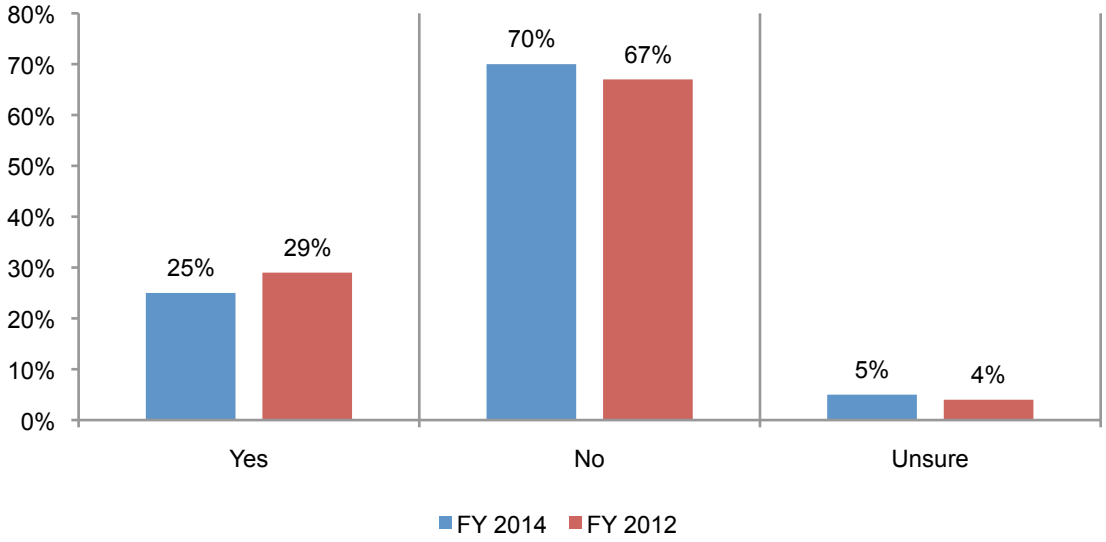
Respondents say most notifications came from credit card companies, retail stores, social media, web retailer, banks and schools & universities, as shown in Figure 3. Since 2012, there were significant increases in notifications from certain industries.

Figure 3. Types of organizations that sent notifications
More than one response permitted



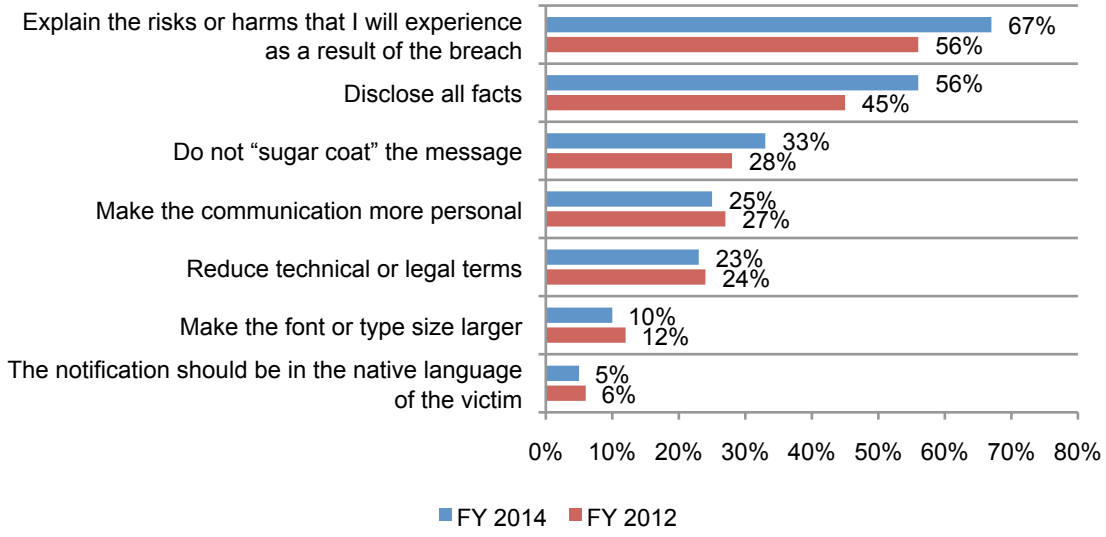
Identity theft protection is not often offered in the notification. As shown in Figure 4, only 25 percent of data breach notifications offered identity theft protection such as credit monitoring or fraud resolution services. This is a slight decrease from 2012 when 29 percent of respondents received such an offer.

Figure 4. Did any of the notifications offer identity theft protection?



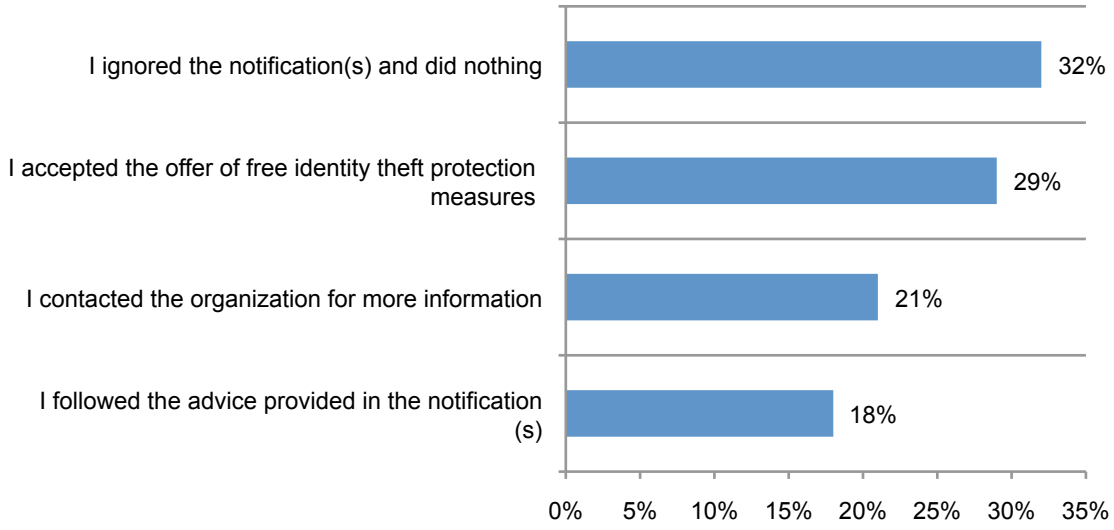
Notifications should focus on facts and what harms are possible. Consumers' sentiments about how data breach notifications can be improved have not changed since 2012. However, respondents are even more adamant that notifications should explain the risks or harms they are most likely to experience as a result of a data breach and disclose all the facts, as shown in Figure 5. They also do not want companies to "sugar coat" the message.

Figure 5. What could the organization do to improve the communication?
Two responses permitted



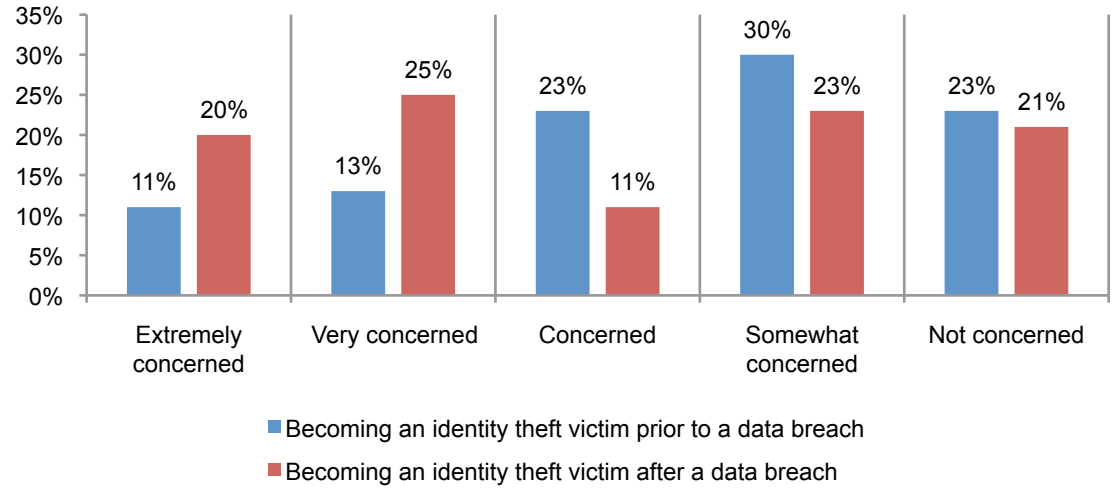
Consumers mostly ignore the notification. The most frequent response to a notification is to ignore it and do nothing (32 percent of respondents) followed by the acceptance of free identity theft protection measures such as credit monitoring or fraud resolution services, as shown in Figure 6.

Figure 6. How did you respond to the notifications you received in the past two years?



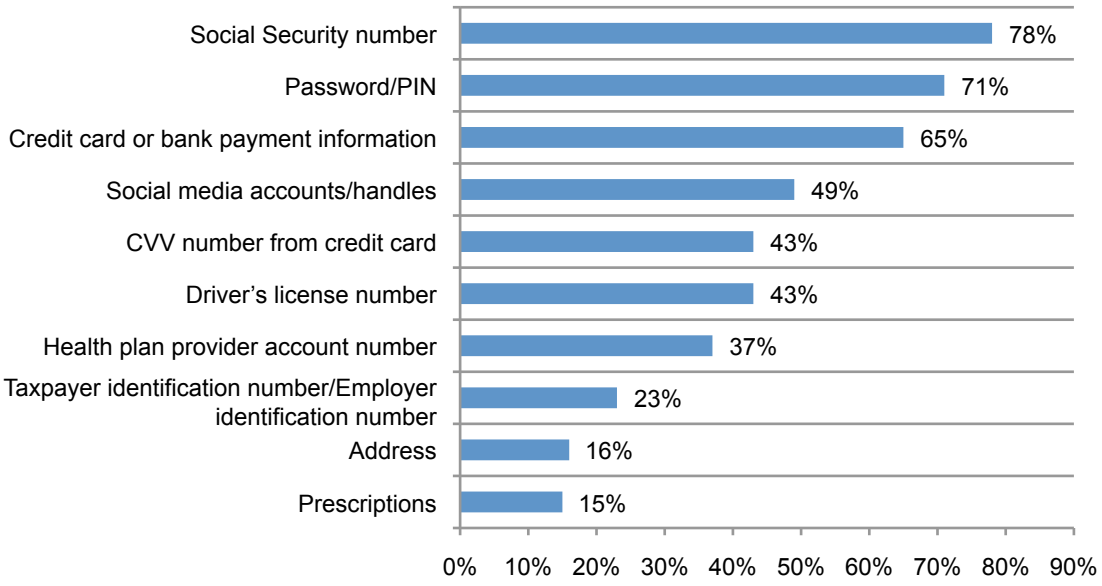
Becoming a victim of a data breach increases fears about becoming an identity theft victim. Prior to having their personal information lost or stolen, 24 percent say they were extremely or very concerned about becoming a victim of identity theft, as revealed in Figure 7. Following the data breach, this concern increased significantly to 45 percent. Forty-eight percent of respondents say their identity is at risk for years or forever.

Figure 7. Concerned about becoming an identity theft victim



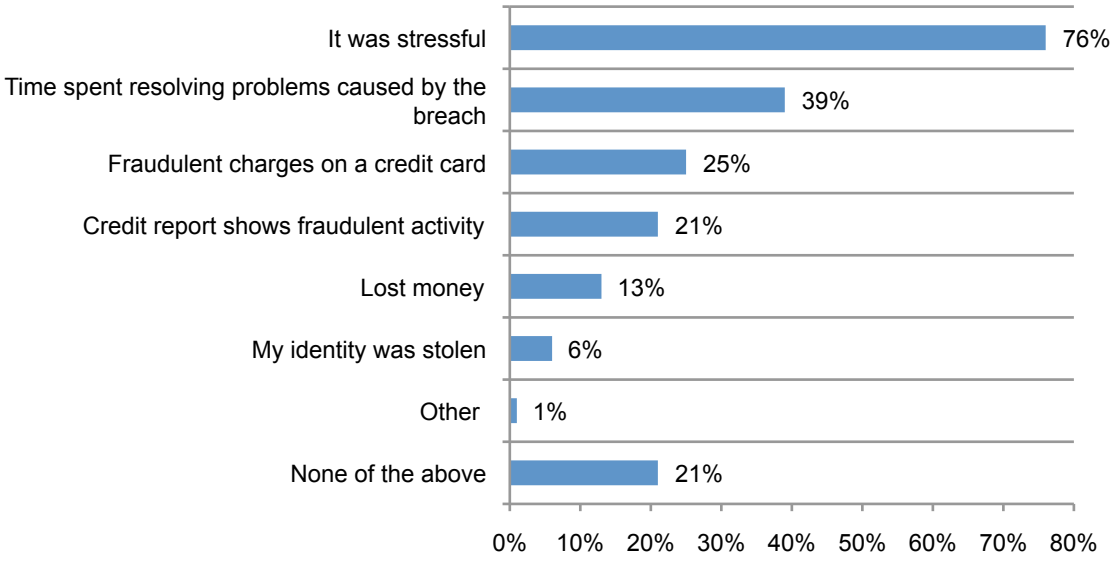
Respondents worry about their Social Security numbers and passwords. While 50 percent say the specific data stolen or lost was their name, 43 percent do not know what personal information was involved in the data breach. Figure 8 reveals the personal data respondents are most concerned about. Seventy-eight percent of respondents say they worry most about having their Social Security number stolen followed by passwords and PIN (71 percent) and credit card or bank payment information (65 percent).

Figure 8. Personal data if lost or stolen would cause the most stress and financial loss
Five responses permitted



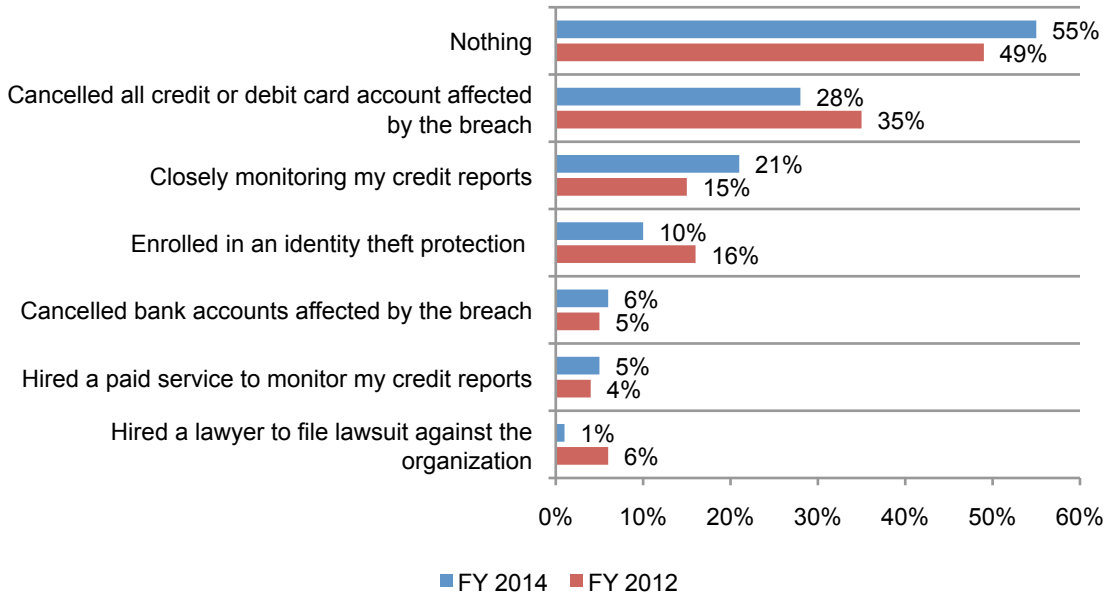
By far, the biggest impact of the data breach was stress (76 percent of respondents). This is followed by having to spend time resolving problems caused by the data breach (39 percent of respondents). Only 6 percent say they found out that their identity was stolen, see Figure 8.

Figure 9. What happened as a result of the data breach?
More than one response permitted



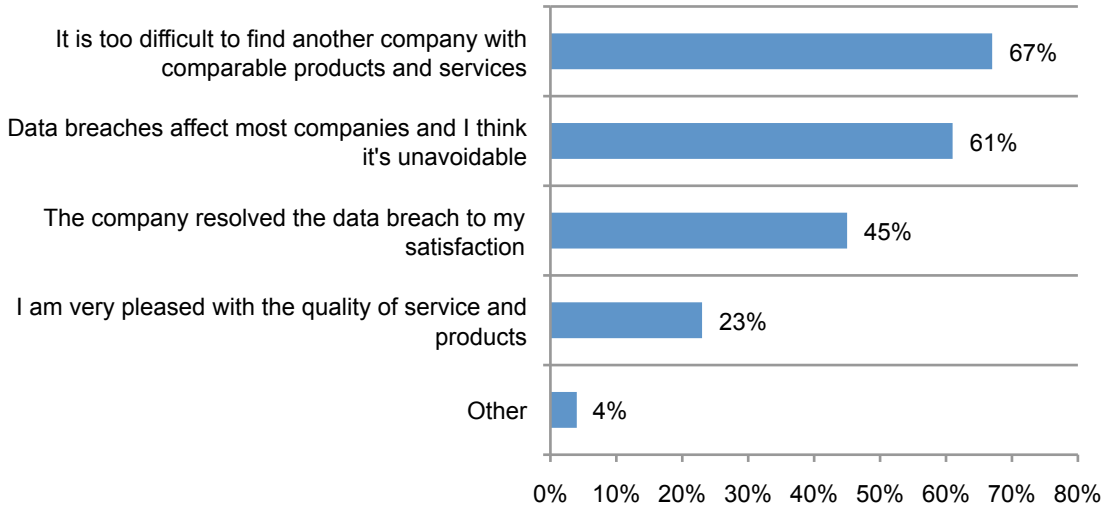
Financial consequences of a data breach are insignificant. Eighty-one percent of respondents who were victims of a data breach did not have any out-of-pocket costs. If they did, it averaged about $38. Thirty-four percent say they were able to resolve the consequences of the breach in one day. Perhaps because the financial consequences are insignificant, 55 percent say they have done nothing to protect themselves and their family from identity theft, as shown in Figure 10.

Figure 10. Steps taken to protect yourself from identity theft
More than one response permitted



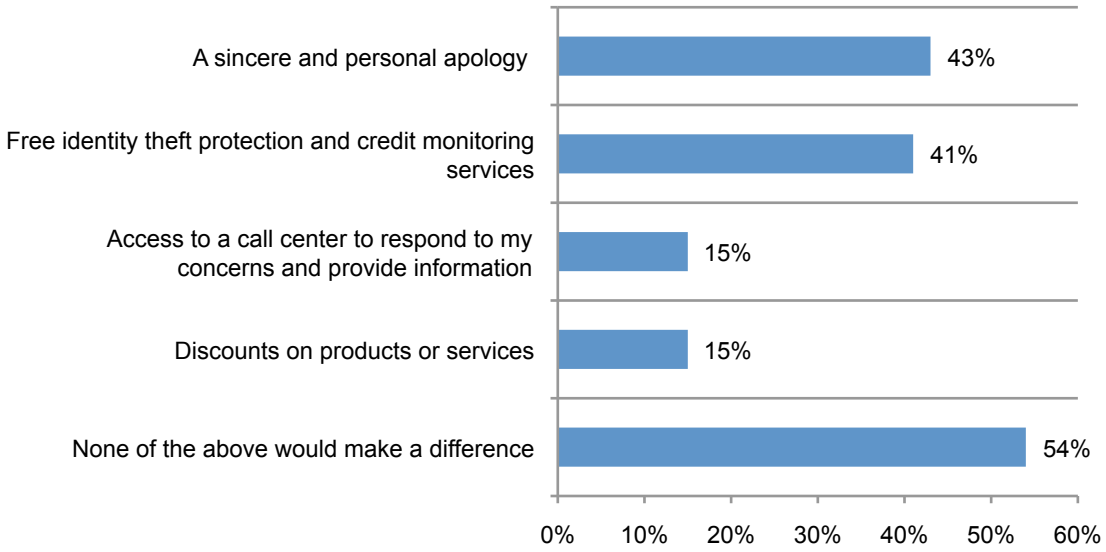
Respondents rarely discontinued their relationship with the company that had a data breach. Seventy-one percent of respondents say they did not leave the company primarily because it is too difficult to find another company with comparable products and services (67 percent of respondents) and data breaches affect most companies and they think it is unavoidable (61 percent of respondents), as shown in Figure 11.

Figure 11. Reasons for continuing a relationship with the company after a data breach
Two responses permitted



What would encourage someone to stay a customer? According to Figure 12, the majority of those respondents (54 percent) who say they discontinued the relationship said nothing would make a difference. This is followed by a sincere and personal apology (43 percent of respondents) and free identity theft protection and credit monitoring services (41 percent of respondents).

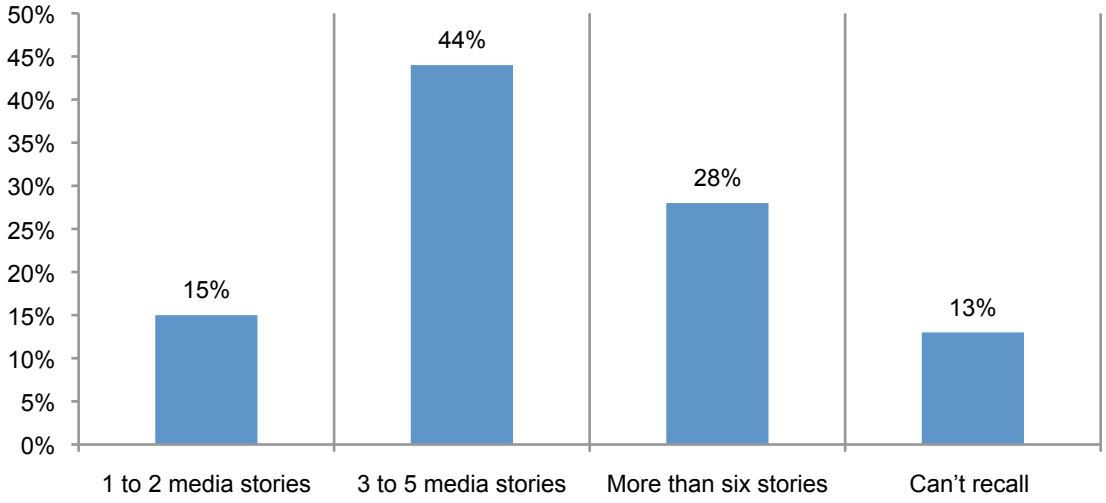
Figure 12. What could be done to prevent you from discontinuing your relationship?
Two responses permitted



The impact of media coverage on consumer sentiment about data breaches

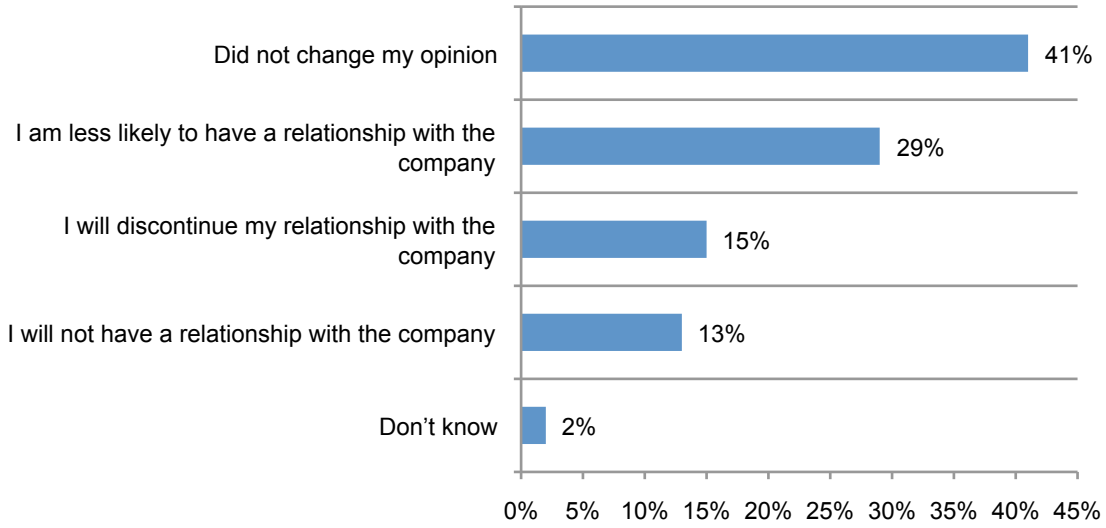
How aware are respondents about media coverage of data breaches? Seventy-two percent of all respondents in this research say that they have heard or read about at least three stories about a data breach reported in the media in the past two years and 13 percent can't recall how many media stories they heard or read about, as shown in Figure 13. The Internet and newspapers are the primary source for the news about data breaches.

Figure 13. How frequently did you hear or read about a data breach reported in the media in the past two years?



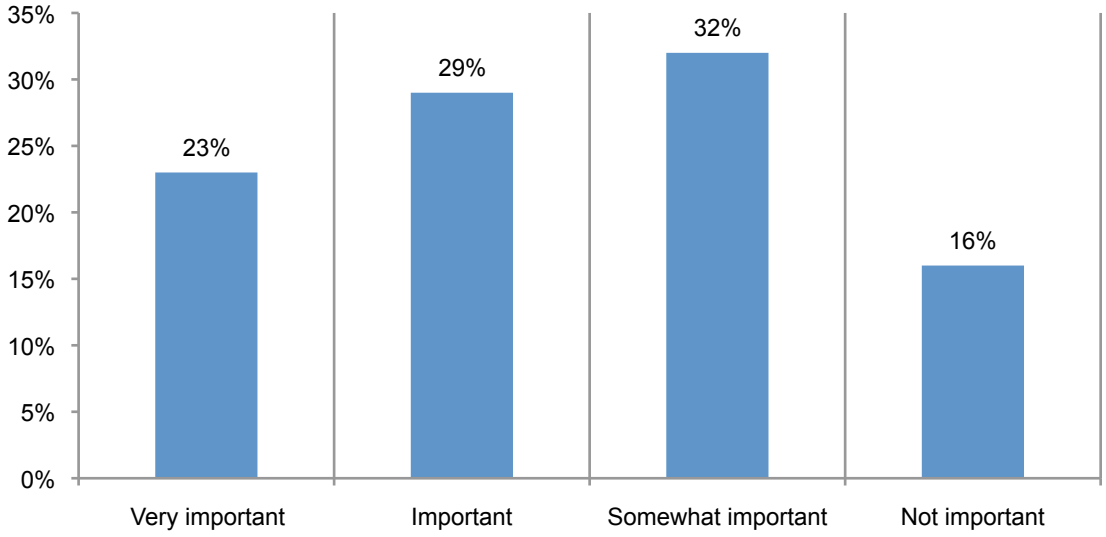
Media coverage about data breaches involving retail stores, social media and credit card companies were the most memorable for respondents. However, 41 percent of respondents reading or hearing about the data breaches say it did not change their opinion about the company, as shown in Figure 13. Only 29 percent say they are less likely to have a relationship with the company.

Figure 13. How did reading about the data breach affect your opinion about the company?



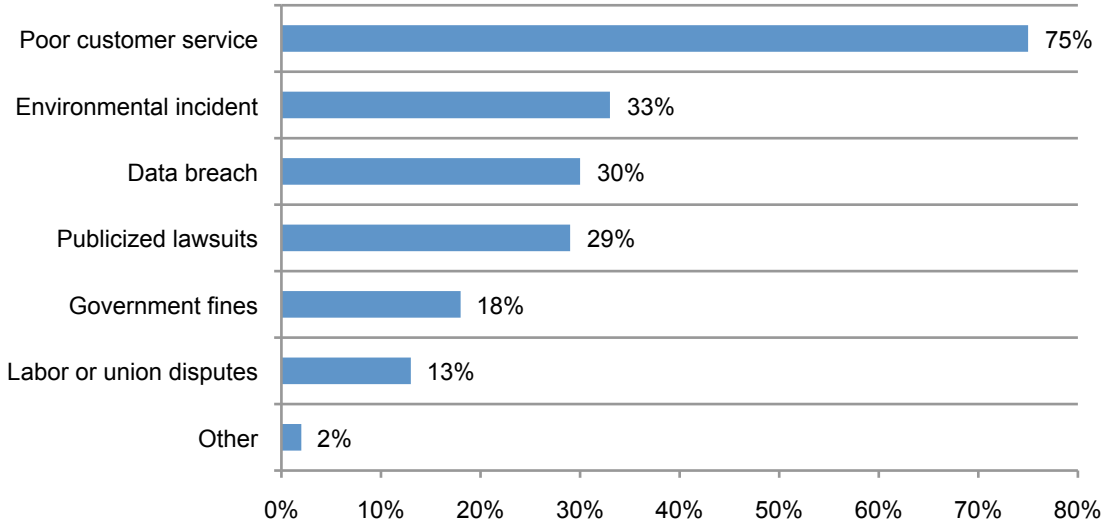
How important is media coverage? According to Figure 14, the majority of respondents believe it is important for the media to report details about data breaches. Mainly because it requires companies to be more responsive to victims followed by the creation of greater awareness about how the data breach could affect individuals and alerts potential victims to take action to protect their personal information from identity theft.

Figure 14. How important is it for the media to report details about data breaches?



What affects reputation most? Data breaches are in the top 3 of incidents that affect reputation. As shown, the biggest reputation spoiler is poor customer service, according to 75 percent of respondents, as shown in Figure 15.

Figure 15. The incident that would have the greatest impact on a company's reputation
Two responses permitted



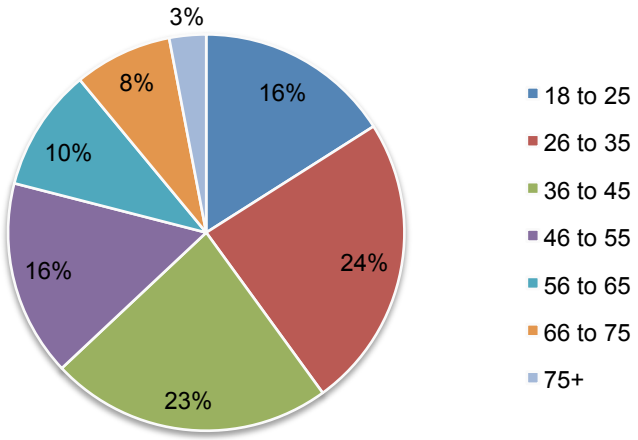
Part 3. Methods

A randomized sampling frame consisting of 20,088 adult-aged individuals who reside within the United States were selected to participate in this survey. A total of 906 respondents completed the survey. Screening and failed reliability checks required us to remove 109 surveys. The final sample includes 797 surveys with a 4.0 percent response rate.

Table 1. Sample response	Freq	Pct%
Sampling frame	20,088	100%
Returned surveys	906	4.5%
Screened or rejected surveys	109	0.5%
Final sample	797	4.0%

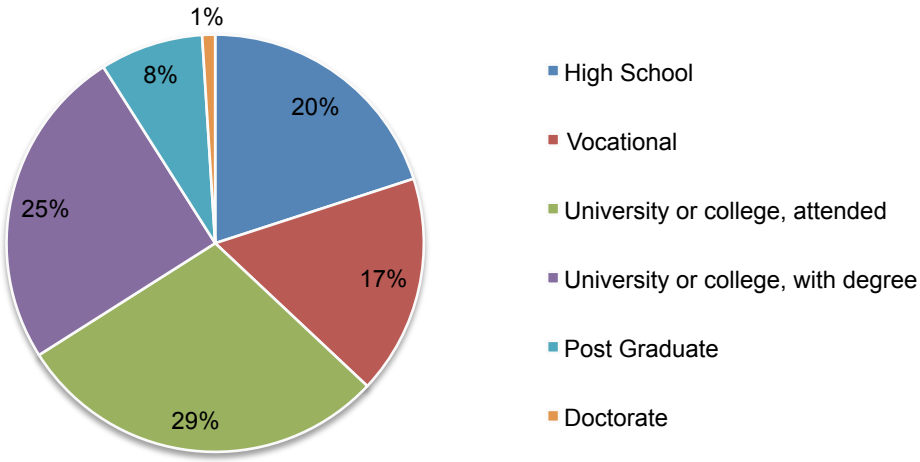
Pie Chart 1 shows 47 present of respondents say they are between the ages of 26 and 45. Eleven percent are above 65 years.

Pie Chart 1. Age range of respondents



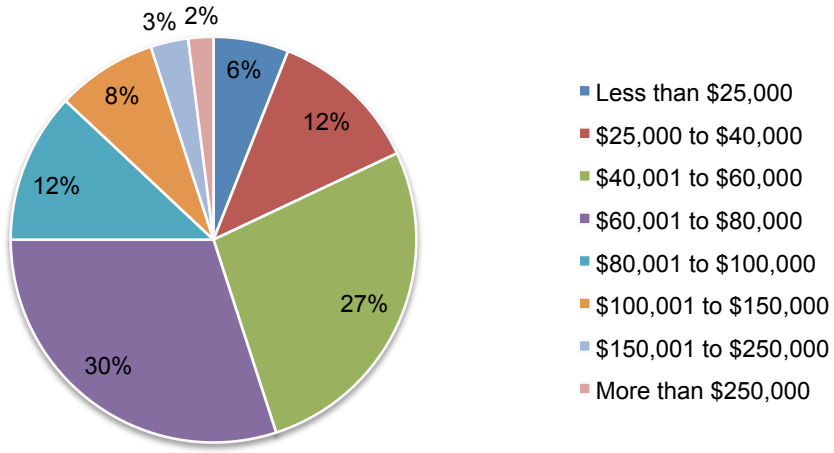
Pie Chart 2 shows 54 percent of respondents say the have attended a university or college. Twenty-five percent say they completed a bachelor's degree.

Pie Chart 2. Highest level of education attained by respondents



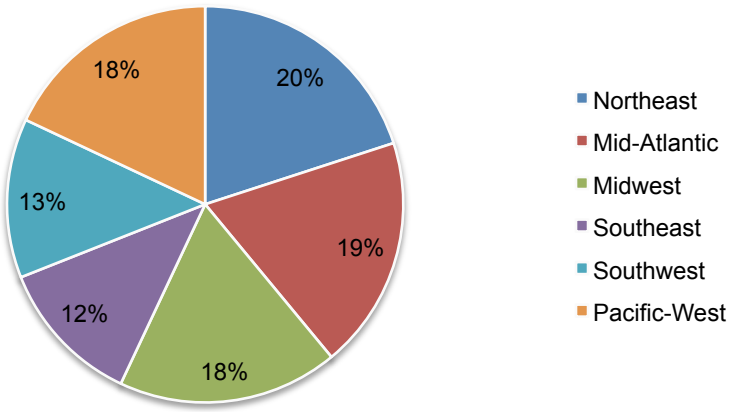
According to Pie Chart 3, 45 percent of respondents say they have household incomes at or below $60,000. Less than 2 percent say their household income is above $250,000.

Pie Chart 3. Annual household income of respondents



Pie Chart 4. U.S. regional location of respondents

Pie Chart 4 shows 20 percent of respondents are located in the Northeast region and 19 percent located in the Mid-Atlantic region. Both the Midwest and Pacific-West regions each represents 18 percent of the sample. The Southeast represents the smallest regional segment at 12 percent.



Part 4. Caveats

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to consumer-based surveys.

- **Non-response bias**: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of adult-aged consumers located in all regions of the United States, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of their underlying beliefs than those who decided to complete the survey.
- **Sampling-frame bias**: The accuracy is based on contact information and the degree to which the sample is representative of individuals who are likely to receive data breach notifications. We also acknowledge that the results may be biased by external events such as media coverage at the time we fielded our survey. Because we used a web-based collection method, it is possible that non-web responses would have resulted in a different pattern of findings.
- **Self-reported results**: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that certain respondents did not provide accurate responses.

Appendix: Detailed Survey Results

The following tables provide the frequency or percentage frequency of responses to all survey questions contained in this study. All survey responses were captured over a six-week period ending in March, 2014.

Part 1: Attributions: Please rate the following statements using the five-point scale provided below each item.	Strongly agree	Agree
Q1. Organizations should be obligated to provide identity theft protection following a data breach involving the loss or theft of my personal information.	31%	32%
Q2. Organizations should be obligated to provide credit-monitoring services following a data breach involving the loss or theft of my personal information.	30%	28%
Q3. Organizations should be obligated to compensate data breach victims with cash, products or services they make.	40%	27%

Part 2. Data breach experience

Q4. Has any organization ever notified you about a data breach that involved your personal information?	FY 2014
Yes	50%
No [Proceed to Part 3]	18%
Cannot recall [Proceed to Part 3]	32%
Total	100%

Only victims of a data breach will respond to the following questions: Q5 to Q20.

Q5. How many data breach notifications as described above, representing different incidents, have you received in the past 2 years?	FY 2014
1	32%
2	30%
3	15%
4	6%
5	7%
More than 5	10%
Total	100%

Q6. Did any of the notifications offer identity theft protection such as credit monitoring or fraud resolution services?	FY 2014
Yes	25%
No	70%
Unsure	5%
Total	100%

Q7. What could the organization do to improve the communication? Please check the top two choices only.	FY 2014
Reduce technical or legal terms	23%
Do not “sugar coat” the message	33%
Make the communication more personal	25%
Disclose all facts	56%
Explain the risks or harms that I will most likely experience as a result of the breach	67%
Make the font or type size larger	10%
The notification should be in the native language of the victim	5%
Other (please specify)	0%
Total	219%

Q8. How did you respond to the one or more notifications you received in the past two years? Please check one response only	FY 2014
I ignored the notification(s) and did nothing	32%
I followed the advice provided in the notification(s)	18%
I contacted the organization for more information	21%
I accepted the offer of free identity theft protection measures such as credit monitoring or fraud resolution services	29%
Total	100%

Q9. Have you been the victim of one of the following mega data breaches? Check all that apply.	FY 2014
Target	33%
Snapchat	2%
Coca-Cola	0%
Michaels	5%
Adobe	22%
LinkedIn	16%
J P Morgan Chase	3%
Twitter	11%
Facebook	16%
Apple	15%
Walgreens	2%
Google Chrome	6%
Nationwide Mutual Insurance	8%
South Carolina Dept of Revenue	9%
Sony	29%
Nieman Marcus	4%
None of the above	34%
Total	215%

Q10. Prior to the data breach(s), how concerned were you that you would become an identity theft victim?	FY 2014
Extremely concerned	11%
Very concerned	13%
Concerned	23%
Somewhat concerned	30%
Not concerned	23%
Total	100%

Q11. Following the data breach(s), how concerned are you that you will now become an identity theft victim?	FY 2014
Extremely concerned	20%
Very concerned	25%
Concerned	11%
Somewhat concerned	23%
Not concerned	21%
Total	100%

Q12. Please indicate the specific data that was lost or stolen? Check all that apply	FY 2014
Name	50%
Address	26%
Email address	22%
Telephone or mobile number	27%
Age/DOB	5%
Driver's license number	1%
Gender	2%
Marital status	1%
Employer	6%
Insurance policy number	6%
CVV number from credit card	15%
Educational background	0%
Credit card or bank payment information	38%
Credit or payment history	9%
Password/PIN	21%
Prescriptions	2%
Social media accounts/handles	15%
Health plan provider account number	10%
Taxpayer identification number/Employer identification number	2%
Social Security number	26%
Other (please specify)	2%
Don't know	43%

Q13. What personal data if lost or stolen in this data breach do you believe would cause you the most stress and financial loss? Please select the top 5 only.	FY 2014
Name	5%
Address	16%
Email address	12%
Telephone or mobile number	6%
Age/DOB	5%
Driver's license number	43%
Gender	1%
Marital status	0%
Employer	11%
Insurance policy number	10%
CVV number from credit card	43%
Educational background	1%
Credit card or bank payment information	65%
Credit or payment history	9%
Password/PIN	71%
Prescriptions	15%
Social media accounts/handles	49%
Health plan provider account number	37%
Taxpayer identification number/Employer identification number	23%
Social Security number	78%
Other (please specify)	0%
Total	500%

Q14. Please indicate the type of organization that reported the data breach to you? Please check all organizations that sent you a notice.	FY 2014
Airline	0%
Bank	16%
Cable Company	0%
Catalogue Merchant	0%
Charitable Organization	6%
Court & Public Records	0%
Credit Card Company	35%
Drug Store	0%
Electric & Gas Utility	0%
Gaming	5%
Grocery Store	8%
Hospitals & Clinics	15%
Hotel	8%
Information Broker	0%
Insurance Company	8%
Internet Service Provider	5%
Financial Advisor	2%
Law Enforcement	0%
Legal & Accounting Firms	0%
Mail or Postal Services	0%
Railways or Bus Line	0%
Retail Store	35%
School & University	16%
Social Media	19%
State & Local Gov Agency	9%
Telephone & Wireless	11%
Travel Agency	0%
Web Retailer	17%
Other (please specify)	2%

Q15. What happened to you as a result of the data breach? Check all that apply.	FY 2014
I found out that my identity was stolen	6%
I have had to spend time resolving problems caused by the breach	39%
I have had fraudulent charges on my credit card	25%
My credit report shows fraudulent activity	21%
It was stressful	76%
I lost money	13%
None of the above	21%
Other (please specify)	1%
Total	202%

Q16. What were your out-of-pocket costs to resolve the consequences of the data breach?	FY 2014
Zero	81%
Less than $10	9%
Between $10 and $50	5%
Between $51 and $100	3%
Between $101 and $500	1%
Between $501 and $1,000	0%
Between $1,001 and $5,000	1%
Between $5,001 and $10,000	0%
Between $10,001 and $25,000	0%
Between $25,001 and $50,000	0%
Between $50,001 and $100,000	0%
Greater than $100,000	0%
Total	100%

Q17. How long did it take to resolve the consequences of the breach?	FY 2014
1 day	34%
1 week	21%
1 month	12%
3 months	4%
6 months	2%
12 months	5%
More than 1 year	7%
Never resolved	15%
Total	100%

Q18. What are you doing to protect yourself from identity theft? Check all that apply..	FY 2014
Nothing	55%
Cancelled all credit or debit card account affected by the breach	28%
Cancelled bank accounts affected by the breach	6%
I am closely monitoring my credit reports	21%
I hired a paid service to monitor my credit reports	5%
I enrolled in an identity theft protection	10%
I hired a lawyer to file lawsuit against the organization	1%
Total	126%

Q19a. Did you discontinue your relationship with the company after the data breach?	FY 2014
Yes	29%
No	71%
Total	100%

Q19b. If yes, what could the company have done to prevent you from discontinuing the relationship? Please select the top two reasons	FY 2014
Free identity theft protection and credit monitoring services	41%
A sincere and personal apology (not a generic notification)	43%
Discounts on products or services	15%
Gift cards	8%
Access to a call center to respond to my concerns and provide information	15%
None of the above would make a difference	54%
Total	176%

Q19c. If no, why did you continue your relationship with the company? Please select the top two reaches	FY 2014
I am very pleased with the quality of service and products	23%
The company resolved the data breach to my satisfaction	45%
Data breaches affect most companies and I think unavoidable	61%
It is too difficult to find another company with comparable products and services	67%
Other	4%
Total	200%

Q20. How long following the data breach do you believe your identity is at risk?	FY 2014
Days	23%
Weeks	14%
Months	15%
Years	22%
Forever	26%
Total	100%

Part 3. Media coverage of data breaches (all respondents)

Q21. How frequently did you hear or read about a data breach reported in the media in the past two years?	FY 2014
None	0%
1 to 2 media stories	15%
3 to 5 media stories	44%
More than six stories	28%
Can't recall how many media stories	13%
Total	100%

Q22. If you heard or read about a data breach in the media, what was the source of the news? Check all that apply.	FY 2014
Radio	19%
Television	39%
Newspapers	40%
Internet	48%
Social media	26%
Total	172%

Q23. After reading about the data breach in the media, how did it affect your opinion about the company?	FY 2014
Did not change my opinion	41%
I am less likely to have a relationship with the company	29%
I will not have a relationship with the company	13%
I will discontinue my relationship with the company	15%
Don't know	2%
Total	100%

Q24. From the list below, please check the types of organizations that you remember had their data breach reported in the media.	FY 2014
Airline	0%
Bank	26%
Cable Company	0%
Catalogue Merchant	0%
Charitable Organization	12%
Court & Public Records	0%
Credit Card Company	44%
Drug Store	2%
Electric & Gas Utility	0%
Gaming	3%
Grocery Store	8%
Hospitals & Clinics	13%
Hotel	16%
Information Broker	4%
Insurance Company	10%
Internet Service Provider	11%
Financial Advisor	2%
Law Enforcement	8%
Legal & Accounting Firms	0%
Mail or Postal Services	0%
Railways or Bus Line	0%
Retail Store	91%
School & University	24%
Social Media	67%
State & Local Gov Agency	39%
Telephone & Wireless	20%
Travel Agency	0%
Web Retailer	60%
Other (please specify)	5%

Q25a. How important is it for the media to report details about data breaches?	FY 2014
Very important	23%
Important	29%
Somewhat important	32%
Not important	16%
Total	100%

Q25b. If important, why?	FY 2014
Provides information about the data breach before the company can notify the victims	11%
Creates greater awareness about how the data breach could affect individuals	54%
Alerts potential victims to take action to protect their personal information from identity theft	53%
Requires companies to be more responsive to victims	67%
Could increase the services and financial compensation to victims	12%
None of the above	30%
Total	227%

Q26. In your opinion, what incident involving a company would have the greatest impact on its reputation? Select the top two.	FY 2014
Poor customer service	75%
Labor or union disputes	13%
Environmental incident	33%
Data breach	30%
Government fines	18%
Publicized lawsuits	29%
Other	2%
Total	200%

Part 4. Demographics

D1. Gender	FY 2014
Female	51%
Male	49%
Total	100%

D2. Age range	FY 2014
18 to 25	17%
26 to 35	23%
36 to 45	23%
46 to 55	16%
56 to 65	9%
66 to 75	8%
75+	4%

D3. Household income range	FY 2014
Less than $25,000	6%
$25,000 to $40,000	12%
$40,001 to $60,000	27%
$60,001 to $80,000	30%
$80,001 to $100,000	12%
$100,001 to $150,000	8%
$150,001 to $250,000	3%
More than $250,000	2%
Total	100%

D4. Highest level of education	FY 2014
High School	19%
Vocational	18%
College (attended, no degree)	28%
College (4 year degree)	25%
Post Graduate	9%
Doctorate	1%
Total	100%

Are you or another member of your immediate family an identity theft victim?	FY 2014
Yes	17%
No	68%
Unsure	15%
Total	100%

Region where you are located	FY 2014
Northeast	19%
Mid-Atlantic	19%
Midwest	17%
Southeast	12%
Southwest	13%
Pacific-West	20%
Total	100%

For more information about this study, please contact Ponemon Institute by sending an email to research@ponemon.org or calling our toll free line at 1.800.887.3118.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.