

Sponsored by



Independently Conducted by



Presents

Consumers' Report Card on Data Breach Notification

Published by Ponemon Institute LLC

April 15, 2008

Consumers' Report Card on Data Breach Notification

Prepared by Dr. Larry Ponemon, April 15, 2008

I. Why is this study important?

It is well established that identity theft has become a very serious issue for Americans.¹ But how well are organizations responding to consumers' worries when their personal information is lost as the result of a data breach?

We decided to conduct this study to find out if consumers who received notification about a data breach involving their personal information were satisfied with the organizations' response and transparency. In other words, if consumers had the ability to issue a report card on the current status of data breach notification would it be A for excellent or F for failing?

Sponsored by ID Experts, Ponemon Institute surveyed 1,795 American consumers to gauge their perceptions, beliefs and concerns after receiving notification about the loss or theft of their personal information from a business or governmental concern. Our survey required consumers who received notification within the past 24 months to express their opinions about the following critical issues:

- Was the organization reporting the data breach responsive and helpful?
- Did the organization's notification quell or inflame fears about the data loss?
- What do consumers think can be done to improve communications about data loss?
- Was the receipt of free or subsidized services helpful? If yes, what services were most valuable to consumers?
- Did the data breach event result in the loss of trust and confidence? If so, what actions did consumers take?

II. Executive summary

This study strongly suggests that legal compliance is the primary goal of many companies' notification efforts. This approach to responding to a data breach does not serve the best interests of consumers and contributes to a breakdown in trust that can impact a company monetarily as a result of an increase in customer defection.

This executive summary highlights the key findings of the study that validate this conclusion. Most prominently, the study found that *63% of survey respondents said notification letters they received offered no direction* on the steps the consumer should take to protect their personal information. As a result, *31% said they terminated their relationship with the organization* and *57% percent said they lost trust and confidence in the organization.*

These data reinforce the conclusion that a poorly executed or confusing data breach response effort can lead to substantial negative consequences for a company including loss of confidence by their customers and significant customer "churn."

The study also found, however, that those individuals in a data breach population that took advantage of a free or subsidized offering, such as credit report monitoring, were *two-and-a-half times more likely* to feel that the company was helpful in responding to their concerns (48% who took advantage of free or subsidized services vs. 19% who either weren't offered these services or didn't take advantage of them). This can lead to lower levels of customer churn and loss of confidence in an organization.

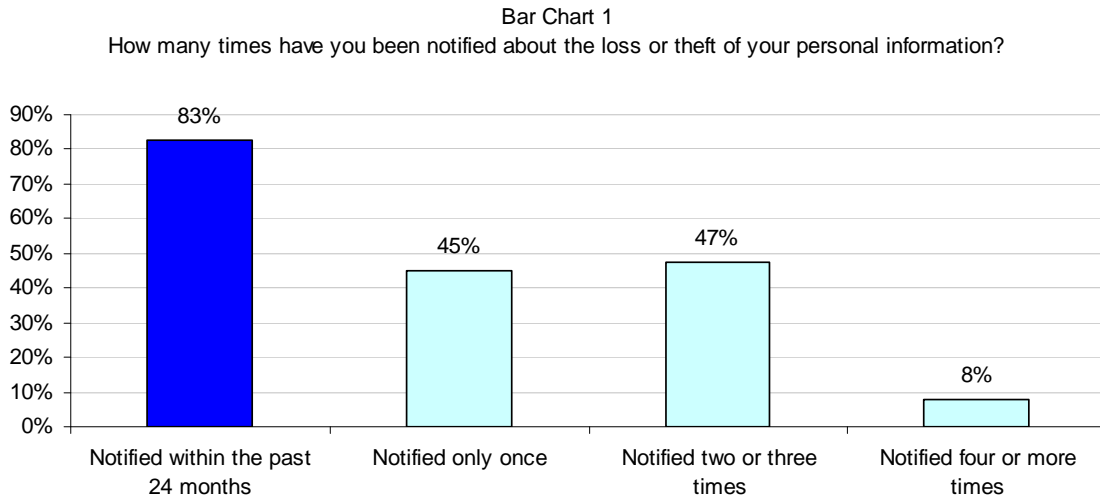
¹Identity theft was by far the largest category of consumer complaints received by the Federal Trade Commission last year. At 32% of all consumer fraud complaints received, identity theft was way ahead of complaints involving shop-at-home/catalog sales (8%) Internet services (5%) and foreign money offers (4%). The FTC estimates that nine million Americans each year are identity theft victims.

Other key findings from this survey include:

- Fifty-five percent of respondents had been notified of two or more data breaches in the previous 24 months, including 8% with four or more notifications;
- More than 55% of respondents state that the notification about the data breach occurred more than one month after the incident, and more than 50% of respondents rated the timeliness, clarity, and quality of the notification as either fair or poor;
- Less than one-third of respondents said that the organization offered services to protect them from further harms; of those who opted into such services, 97% rated them good to excellent; and,
- Two percent of respondents who had been notified of a data breach experienced identity theft as a result of the breach, while 64% were unsure if they were a victim of identity theft.

Following are the top ten findings of this study supported by a chart illustrating the data.

1. Over 83% of survey respondents said they received one or more data breach notifications over the past 24 months.



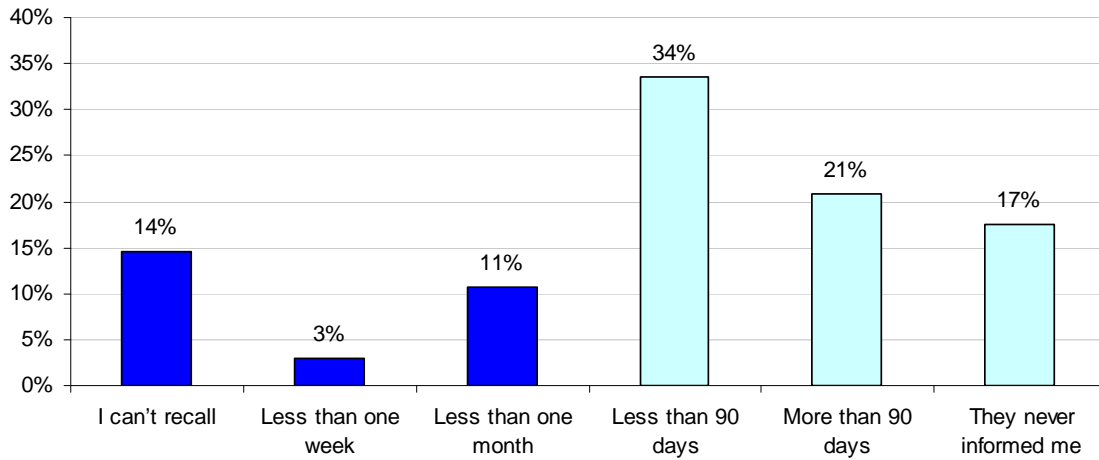
Bar Chart 1 reports the frequency of data breach for a subsample of respondents who received notification. As can be seen, more than half received two or more data breach notifications, and 8% reported that they received four or more notifications in the past two years.

It is interesting to note that the majority of breach incidents involved the loss or theft of customer or consumer data (52%). Another 18% involved the loss of employee information, and 16% pertained to the loss of taxpayer, citizen or veteran information by a governmental organization. Only 6% of breach incidents involved students or patients.

2. Fifty-five percent of respondents received the data breach notification more than one month after the incident.

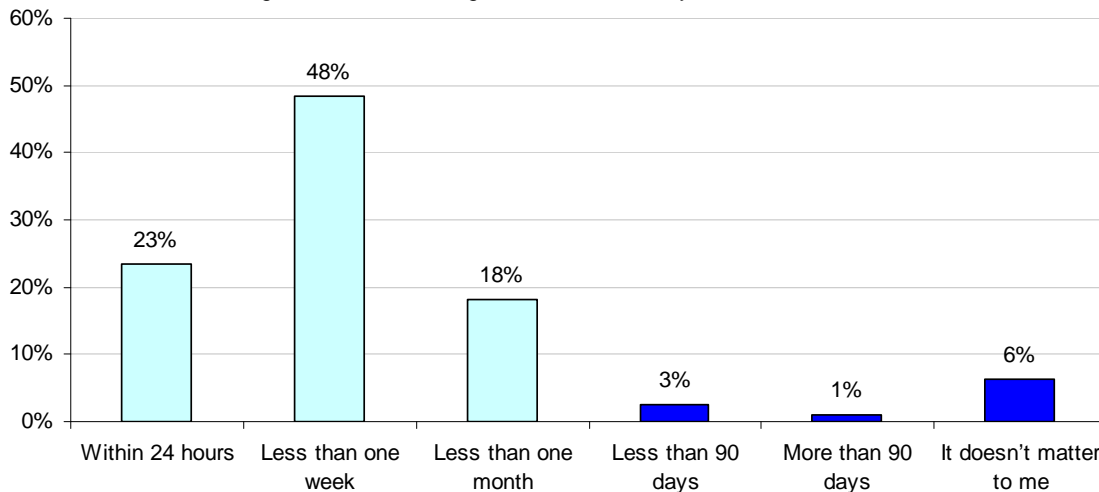
Bar Chart 2a reports the time delay between the data breach incident and the date respondents recall receiving their notification about the breach event. As shown, 34% of respondents received notification more than one month but less than 90 days following the incident. Another 21% recalled receiving notification after 90 days. Seventeen percent said they never received formal notification about a data breach that occurred.

Bar Chart 2a
How long after the data breach before the organization contacted you?



Bar Chart 2b reports the frequency of respondents according to their beliefs about how long the required notification should occur after discovery of a data breach event. As shown, 71% of respondents believe notice should occur less than one week after the incident. In contrast to actual experience reported in Bar Chart 2a, only 10% of respondents believe that more than one month is an acceptable time delay after the incident.

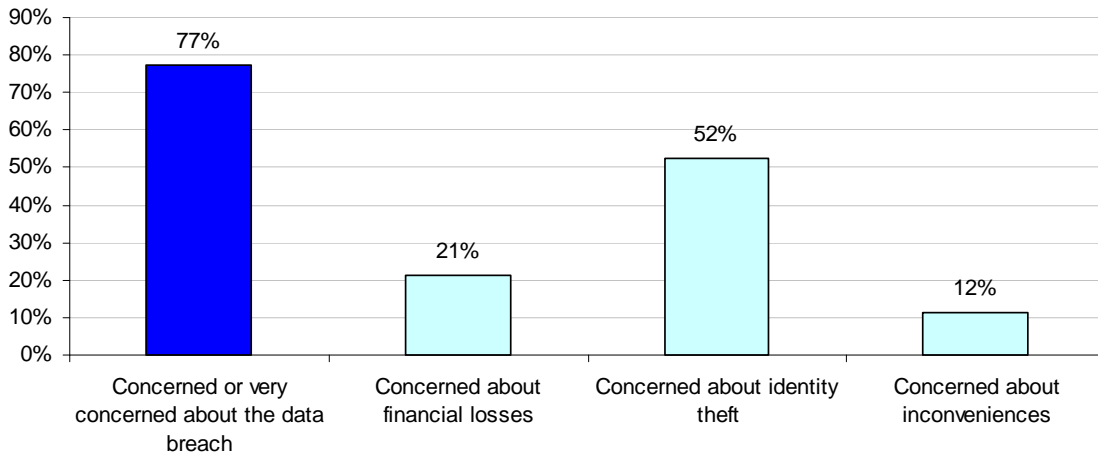
Bar Chart 2b
How long should it take an organization to contact you about a data breach?



3. Seventy-seven percent of respondents are concerned or very concerned about loss or theft of their personal information.

According to Bar Chart 3, 52% of respondents say that their number one concern is identity theft. Another 21% worry about financial losses. Another 12% express concern about having to transfer their business to another organization.

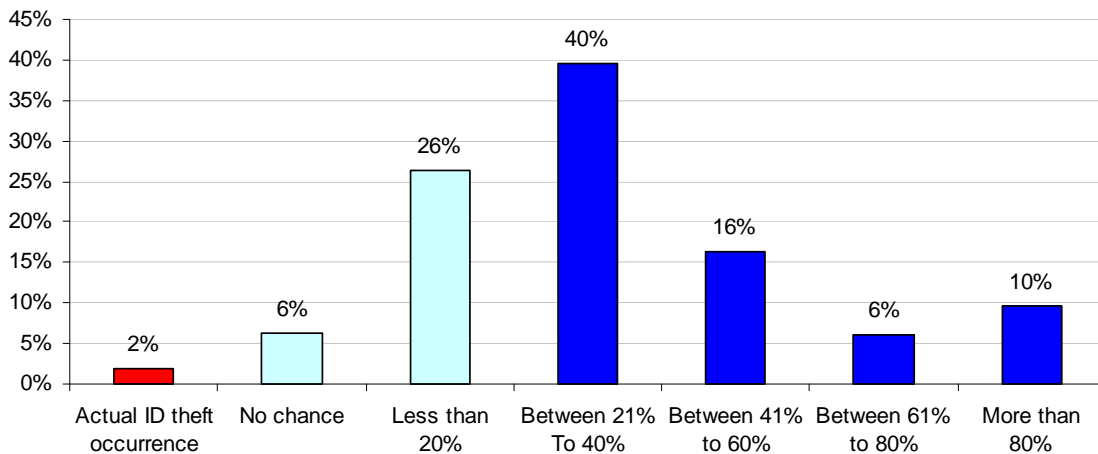
Bar 3
Respondents' concerns about data breach



4. A large number of respondents believe they may become victims of identity theft as a result of the data breach incident.

Bar Chart 4 shows that 72% believe their chances of becoming an identity theft victim is greater than 20%. Approximately 32% believe that the likelihood of becoming an identity theft victim is greater than 40%

Bar Chart 4
What is the likelihood that you will become a victim of identity theft?



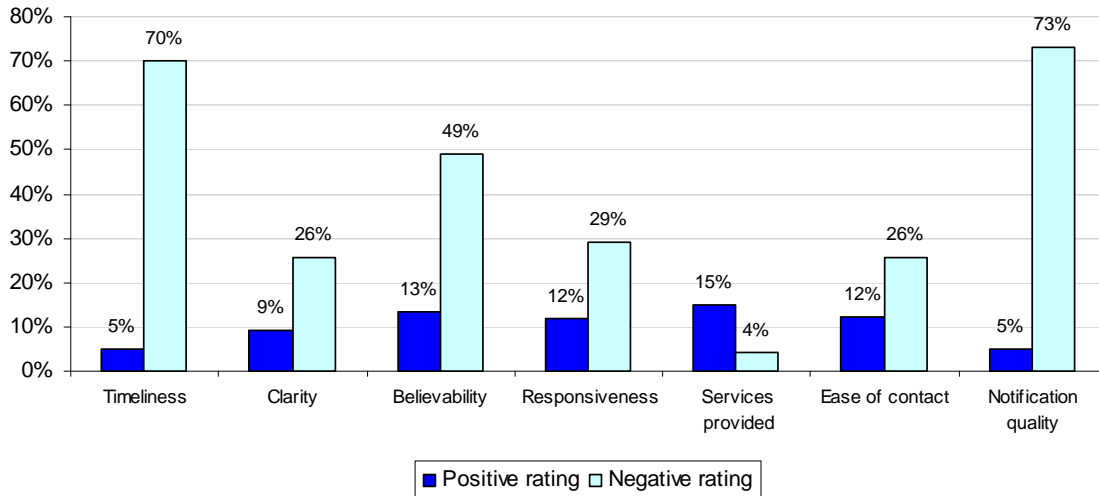
Despite these concerns, less than 2% of respondents said they became a victim of an identity theft crime as a result of the data breach incident. In other words, consumers' fears about the possibility of becoming an identity theft victim do not reflect the actual rate of experience.

5. The vast majority of respondents believe that the organization's notification of the data breach was poorly executed.

Bar Chart 5 compares seven features of the data breach notification. Clearly very few respondents rated their experience as excellent or very good. Accordingly, less than 10% of respondents rated timeliness of the notification, clarity of the communication, and quality of the communication as excellent or very good (positive rating). In contrast, more than 50% of

respondents rated the timeliness of communication, clarity of the communication and quality of the notification as either fair or poor (negative rating).

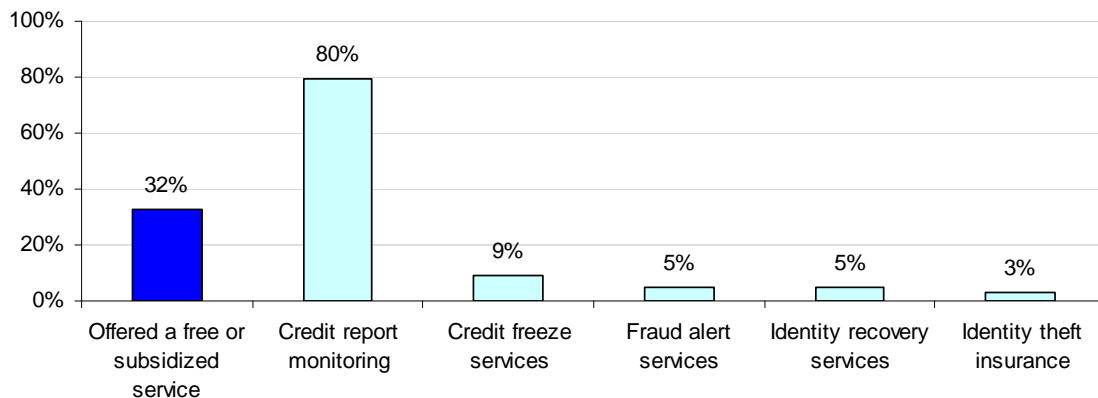
Bar Chart 5
Respondents' rating of the data breach notification process



6. Less than 32% of respondents said that the organization reporting the data breach offered services to protect them from further harms.

For those respondents receiving free or subsidized services, about 80% said credit monitoring was offered. Another 9% were offered credit freeze services. The remaining services included fraud alerts (5%), identity recovery (5%) and identity theft insurance (3%). These results are shown below.

Bar Chart 6
Respondents offered a free or subsidized service to minimize potential harms

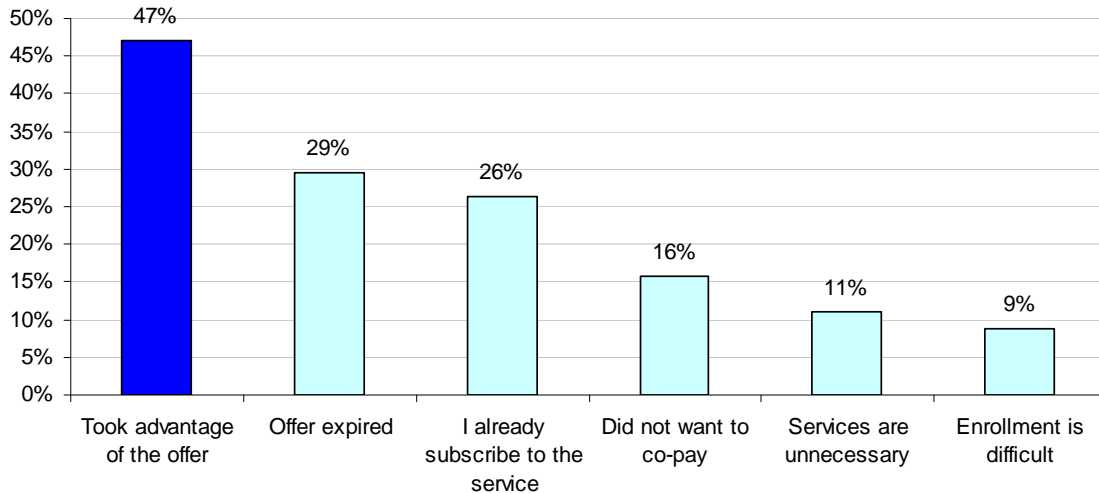


7. Less than 47% of respondents said that they took advantage of the free or subsidized services offered by the organization reporting the data breach.

For those respondents who did not take advantage of the free or subsidized services, why not? Bar Chart 7 shows that 29% became ineligible because of responding too late. Another 26% already had the free or subsidized service offered by the company. About 16% said they did not

want to co-pay for the subsidized service, and 11% did not believe the service was necessary or helpful.

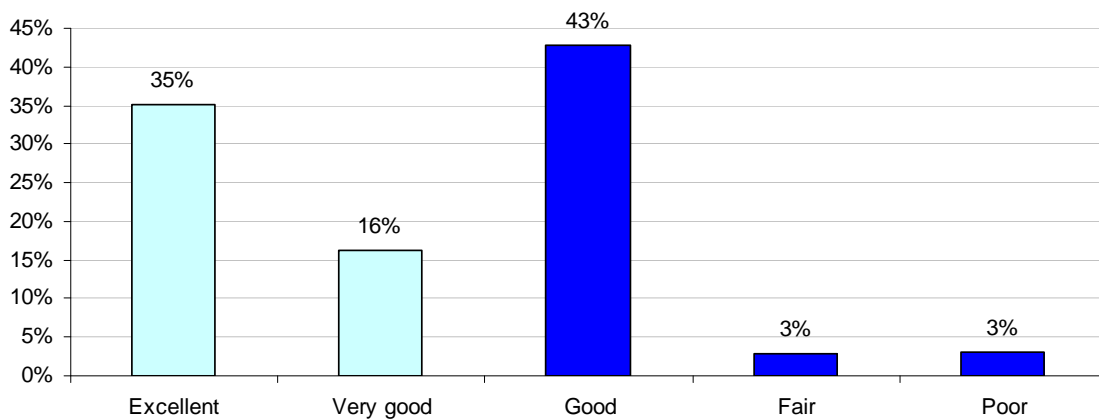
Bar Chart 7
Why did you not take advantage of the free or subsidized service?



8. A majority of respondents who elected to receive free or subsidized services reported that they found them helpful and of high quality.

Bar Chart 8 reports the perception of respondents who took advantage of the offer to receive a free or subsidized service. Thirty-five percent believe that these services were excellent. Another 16% rated these services as very good, and 43% said services were good. Only 6% rated the free or subsidized service as fair or poor.

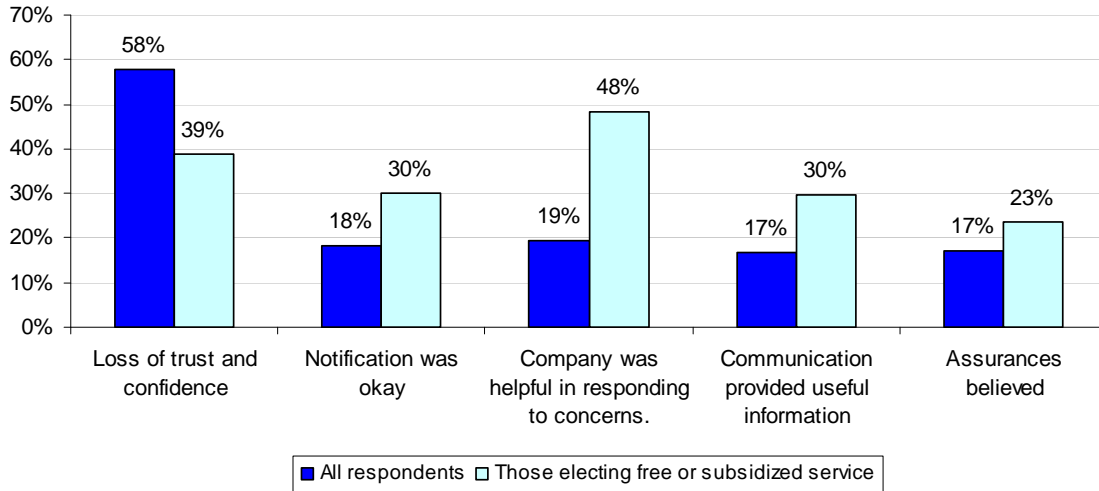
Bar Chart 8
How consumers perceive the quality of free or subsidized services



9. Respondents' opinions about the organizations overall performance in handling the data breach incident appears to be related to free or subsidized services received by them.

Bar Chart 9 provides the summarized results of survey questions that captured respondents' perceptions about the organization notifying them about the loss or theft of their personal information. Over 57% of all respondents either agree or strongly agree that the data breach caused them to lose trust and confidence in the organization.

Bar Chart 9
Differences in perceptions and beliefs among all respondents in comparison to those electing to receive a free or subsidized service

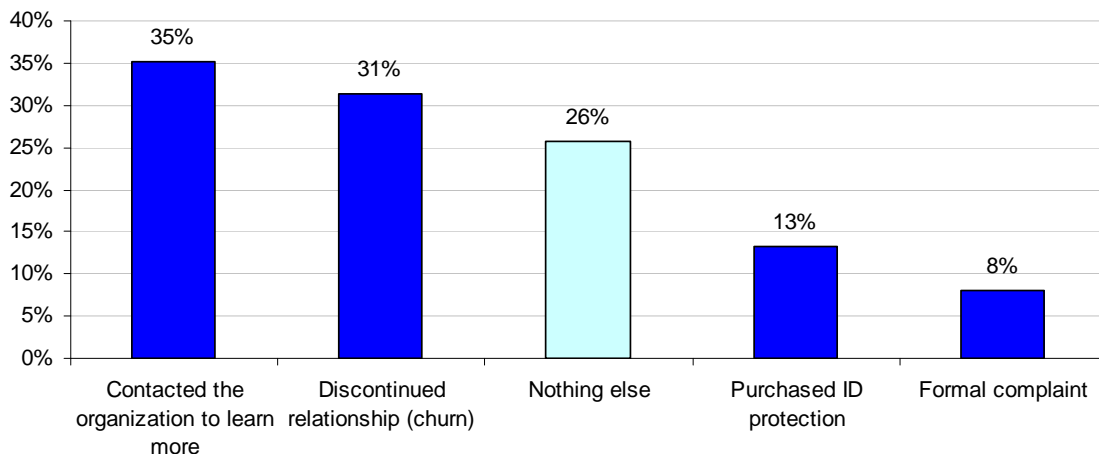


However, only 38% of respondents who received free or subsidized services held this belief. Similarly, while less than 18% of respondents believed the organization did a good job in handling the breach, over 30% of respondents who took advantage of free or subsidized services felt this way. Other differences between the overall sample and the sub-sample of respondents who took advantage of free or subsidized services are also revealed.

10. The most common actions taken by respondents after being notified about the data breach was to directly contact the organization reporting the breach or to discontinue a relationship with the organization (i.e., churn).

As shown in Bar Chart 10, over 35% stated that the immediate response after receiving notification about the data breach was to contact the organization directly. Another 31% reported that they discontinued their relationship with the organization. Over 26% of respondents said they did nothing after learning about the breach event, and 13% said they contacted the organization to purchase services to protect their privacy.

Bar Chart 10
What was the respondent's response to data breach



III. 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 most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of individuals, 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 underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of American consumers. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a Web-based collection method, it is possible that non-Web responses by mailed survey or telephone call would result 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 a subject did not provide a truthful response.

IV. Sample

Table 1 reports the sample characteristics. We asked 27,998 adult-aged Americans to participate in this web survey. Our randomly selected sampling frame was balanced against US national census demographics. In total, 1,998 respondents completed their survey results during within an 11-day research period. Of returned instruments, 203 survey forms were rejected because of reliability checks. A total of 1,795 surveys were analyzed in our final sample. This sample represents a 6.4% net response rate. The margin of error on all adjective scale and Yes/No/Unsure responses is $\leq 3\%$.

Table 1: Sample characteristics	Freq.	Pct%
Sampling frame	27998	100.0%
Bounced back	1008	3.6%
Total response	1998	7.1%
Rejected surveys	203	0.7%
Final sample	1795	6.4%

Over 90% of respondents completed all survey items within 12 minutes. Following are key demographics survey respondents. Table 2a reports the age range of respondents and Table 2b provides the self-reported range of household income. As can be seen, a majority of respondents are less than 46 years of age and earn income levels below \$61,000.

Table 2a Age range	Pct%
18 to 25	20%
26 to 35	24%
36 to 45	26%
46 to 55	16%
56 to 65	6%
66 to 75	5%
75+	3%
Total	100%

Table 2b Approximate household income	Pct%
Less than \$20,000	23%
\$20,000 to \$40,000	25%
\$41,000 to \$60,000	32%
\$61,000 to \$80,000	7%
\$81,000 to \$100,000	5%
\$101,000 to \$150,000	4%
\$151,000 to \$200,000	1%
\$201,000+	1%
Total	100%

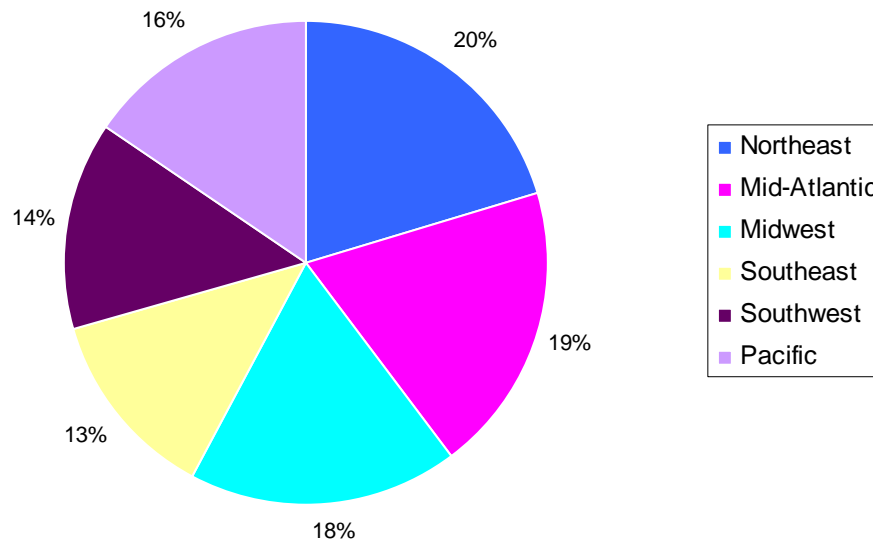
Table 3a shows the self-reported head of household status, and Table 3b indicates gender. A majority of respondents report they are head of household and are female – both representing 51% of the total sample.

Table 3a	
Are you the head of your household?	Pct%
Yes	51%
No	49%
Total	100%

Table 3b	
Gender	Pct%
Male	49%
Female	51%
Total	100%

Pie Chart 1 reports the distribution of respondents by region of the United States. As shown, they represent all major regions of the country with 45 states included. The northeast region represents the largest number of respondents (20%), and the southwest region represents the smallest number of respondents (13%).

Pie Chart 1: Geographic regions of the United States



Pie Chart 2 reports how respondents perceive the importance of their privacy rights. Over 87% of these individuals say that the protection of their privacy is either “very important” or “important” to them. Only 8% say that the protection of their privacy rights is “irrelevant,” and less than 5% say it is “not important.”

Pie Chart 2
How important to you is the protection of your privacy rights?

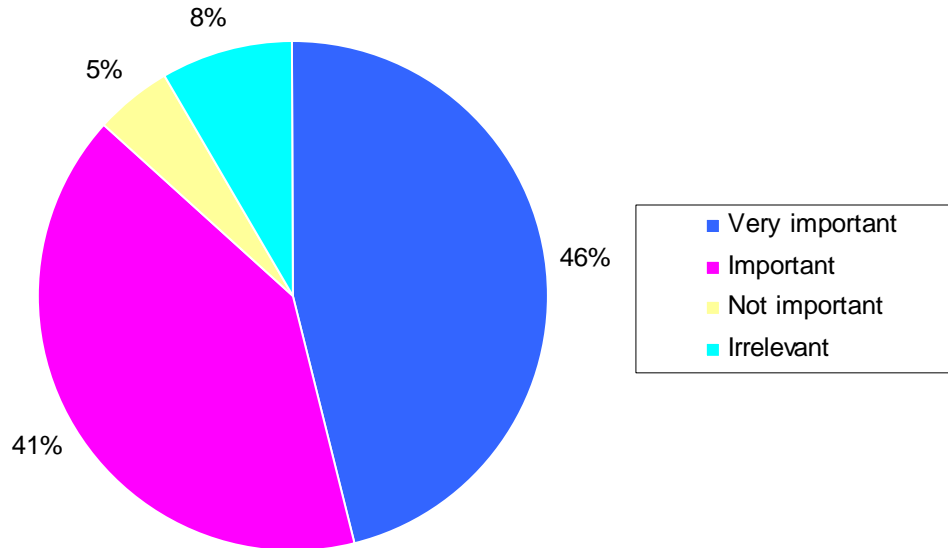


Table 4a reports the highest level of education attained by respondents. The majority of individuals have a high school or vocational school education. Table 4b provides the self-reported employment status of respondents. As can be seen, 54% of respondents are presently employed in a full-time position.

Table 4a Highest level of education attained	Pct%
High School	31%
Vocational	28%
College (4 yr)	32%
Post Graduate	8%
Doctorate	1%
Total	100%

Table 4b: Employment status	Pct%
Full time employee	54%
Part time employee	15%
Owner/partner of business	10%
Independent contractor	3%
Retired	9%
Unemployed	2%
Student	6%
Total	100%

V. Report Card

The first *Consumers' Report Card on Data Breach Notification* gives business and governmental organizations less than a passing grade. In fact, consumers affected by a data breach are failing organizations on their performance in the following areas:

- **Responsive and helpful notification**

Consumers affected by a data breach do not believe organizations' responsiveness and helpfulness in the notification of a data breach is appropriate. Specifically, the actual communication did not provide guidance in understanding or managing information risks associated with the loss or theft of their personal data. In addition, they believe it took too long to receive the notice and when they did receive the notification it did not provide enough information about the breach.

- **Reassurance about protection of personal information**

Consumers do not trust the messages conveyed within the notification or public disclosure about the data breach incident. Many believe the communications were unbelievable, missing key facts and lacking credibility. The pattern of these findings suggests that the notifications were inadequate in reducing consumers' fear about potential harms they face as a result of this incident.

- **Communications**

In general, consumers have consistent perceptions about how the data breach notification process can be improved. The main areas of improvement include: (1) prompt disclosure with minimal lag between incident discovery and public reporting, (2) clear and concise description about potential harms and remedies available to curtail harm, and (3) support services such as credit report monitoring, identity protection services, or identity theft insurance that reduce or mitigate harm.

- **Access to free or subsidized services**

Our findings also suggest that identity protection services are viewed as very helpful for reducing fears or concerns about identity theft and other related information or cyber crimes. Specifically, individuals who received free or subsidized support services maintained a more positive perception about the organization reporting the breach than those who did not use these services. In addition, individuals receiving services are less likely to churn or express turnover intentions as a result of the data loss or theft. Despite clear benefits to organizations, a majority of consumers said they did not receive an offer for free or subsidized identity support services.

- **Trust and confidence in the organization**

We found that organizations reporting the breach often experienced an immediate loss of confidence by those individuals receiving the notification. Obviously, the best way to maintain consumers' trust is to avoid a data breach in the first place with safeguards that will secure customer and employee data from loss or theft. In the event a data breach occurs, an organization's incident response plan should focus on providing timely notification to consumers that is easily understood and explains what is being done to protect their information from further harm. The notification should also include information about available services and guidance on how they can protect themselves from identity theft. We believe that these measures will help improve the failing grades consumers are giving to how organizations currently are responding to data breaches.

The following appendix reports the percentage frequencies of all survey questions included in our survey instrument.

Appendix: Percentage Frequency Survey Responses

Q1a. Have you received one or more data breach notifications concerning the loss or theft of your personal information from a business, educational or governmental organization in the past 24 months?	Pct%
Yes	83%
No	17%
Total	100%

Q1b. How many times in the past 24 months did you receive a notification concerning the loss or theft of your personal information?	Pct%
Once	45%
Two or three times	47%
Four or more times	8%
Total	100%

Q1c. Did you experience identity theft as a result of a data breach?	Pct%
Yes	2%
No	34%
I don't know	64%
Total	100%

If you received more than one notification, please refer to the most recent event when answering the remaining questions in this survey.

Q2. How were you notified? Please select all that apply.	Pct%
Personal letter addressed to me from the company or organization	67%
Personal letter from a third-party such as an outside law firm	6%
Notification included in a statement or bill	10%
Phone call from the company or organization	15%
Phone call from a third party	4%
E-mail message	5%
Disclosure on organization's website	5%
Disclosure in newspaper or on television	12%
Other (please specify)	14%
Total	136%

Q3a. Approximately how long after the data breach did it take for the organization to inform you? Please select only one.	Pct%
I can't recall	14%
Less than one week	3%
Less than one month	11%
Less than 90 days	34%
More than 90 days	21%
They never informed me	17%
Total	100%

Q3b. Approximately how soon do you think you should have been notified following the data breach?	Pct%
Within 24 hours	23%
Less than one week	48%
Less than one month	18%
Less than 90 days	3%
More than 90 days	1%
It doesn't matter to me	6%
Total	100%

Q4. What best describes the timing of the data breach notification you received? Please select only one.	Pct%
I learned about the data breach directly from the organization before hearing about it in the media or from other sources.	44%
I learned about the data breach directly from the organization after hearing about it in the media or from other sources.	46%
I learned about the data breach from the organization and the media (or other sources) at the same time.	11%
Total	100%

Q5a. What best describes the information about you that was lost or stolen in this data breach? Please select only one.	Pct%
Customer/consumer	52%
Employee	18%
Patient	6%
Student	6%
Taxpayer/citizen/veteran	16%
Other (specify)	1%
Total	100%

Q5b. What best describes the organization that had the data breach? Please select only one.	Pct%
Financial institution or credit card company	30%
Retailer	23%
Online merchant	10%
Health care provider	6%
Educational institution	9%
Governmental organization	16%
Telecom or cable company	4%
Other (please specify)	4%
Total	100%

Q6. What was the cause of the data breach?	Pct%
Theft by a hacker or criminal outside the company	2%
Theft by a malicious insider such as an employee or contractor	0%
Lost laptop or other portable data-bearing device by the organization	19%
Lost laptop or other portable data-bearing device by a third party	15%
Mishaps in the transmission of electronic information	1%
Mishaps in the movement of paper (manual) information	7%
Lost backup files or tapes	2%
I do not know the cause of the data breach	50%
Other (please specify)	4%
Total	100%

Q7a. What best describes your level of concern after learning about the loss or theft of your personal information?	Pct%
Very concerned	39%
Concerned	38%
Somewhat concerned	16%
Not concerned	7%
Total	100%

Q7b. If concerned, why? Please select the top two reasons.	Pct%
Financial losses	21%
Possible theft of my identity	52%
Revelation of extremely confidential information	6%
My data will be available to aggressive marketers	3%
I will need to spend time correcting errors to my records	6%
I will need to transfer my business to another organization	12%
Other	0%
Total	100%

Q8. If you have not as yet experienced identity theft as a result of the data breach, do you believe that the loss of your information will ultimately result in your identity being stolen? If yes, what do you think is the chance or probability that this will occur?	Pct%
Zero (no chance of occurrence)	6%
Between 0 to 20%	26%
Between 21 To 40%	40%
Between 41 to 60%	16%
Between 61 to 80%	6%
Between 81 to 100%	5%
Total	100%

Q9a. What was your response after learning about the data breach? Please select all that apply.	Pct%
I contacted the organization to learn more about the incident	35%
I discontinued my relationship with the organization	31%
I made a formal complaint to the organization	8%
I contacted a consumer advocate organization such as the Better Business Bureau	2%
I contacted my state or local government	2%
I contacted an agency of the federal government such as the Federal Trade Commission	0%
I contacted my attorney	2%
I contacted an organization to purchase services to protect my personal information	13%
Nothing	26%
Other	2%
Total	122%

Q9b. If you did nothing, what was the reason? Please select only one response.	Pct%
I did not have time	10%
The data breach notification did not give me any guidance as to what I should or could do to protect my personal information	63%
I did not understand what services would be available to help me	4%
The services offered to me by the organization that lost my personal information required me to disclose personal information such as a Social Security number	11%
I was not concerned about how the data breach would affect my personal information	8%
Other	3%
Total	100%

Please rate each one of the following four statements using the scale provided below.

Q10a. The data breach caused me to lose trust and confidence in the organization	Pct%
Strongly agree	35%
Agree	22%
Unsure	21%
Disagree	19%
Strongly disagree	2%
Total	100%

Q10b. The organization did a good job in notifying me about the data breach.	Pct%
Strongly agree	8%
Agree	10%
Unsure	17%
Disagree	20%
Strongly disagree	45%
Total	100%

Q10c. The organization was helpful to me in responding to my concerns.	Pct%
Strongly agree	6%
Agree	14%
Unsure	16%
Disagree	29%
Strongly disagree	36%
Total	100%

Q10d. The organization's communication provided useful information on simple things I could do to protect myself from identity theft.	Pct%
Strongly agree	6%
Agree	11%
Unsure	19%
Disagree	21%
Strongly disagree	43%
Total	100%

Q10e. The organization assured me that any harms would be minimal .	Pct%
Strongly agree	3%
Agree	14%
Unsure	21%
Disagree	33%
Strongly disagree	29%
Total	100%

Q11. Please rate the following seven features of the data breach notification event using the following scale: 1=excellent, 2 = very good, 3 = good, 4 = fair and 5 = poor, 9 = not applicable						
	1	2	3	4	5	9
Timeliness of the notification	1%	4%	12%	36%	34%	12%
Clarity of the communication	1%	8%	43%	16%	10%	21%
Believability of the communication	2%	11%	33%	29%	21%	5%
Responsiveness to my questions or concerns	4%	8%	13%	18%	11%	46%
Services provided to minimize harm	4%	11%	14%	1%	3%	67%
Ease in contacting organization	4%	9%	17%	13%	12%	45%
Quality of the notification communication about the data breach	1%	4%	13%	34%	39%	9%
Average	2%	8%	21%	21%	19%	29%

Q12. There are several services now available to help individuals protect themselves when their personal information has been lost or stolen. Please rate your understanding of five types of services that an organization might offer you using the following scale: 1=I understand what this service is and how it will benefit me; 2=I don't understand what this service is or how it might benefit me	1	2
Credit freeze services	38%	62%
Credit report monitoring services	58%	42%
Fraud alert services	55%	45%
A copy of your credit report from one or more credit bureaus	60%	40%
Identity theft insurance	47%	53%
Identity recovery services (if your identity is stolen)	29%	71%
Average	48%	52%

Q13a. Did the organization offer you any of the above services to protect you from further harms?	Pct%
Yes	32%
No	68%
Total	100%

Q13b. If yes, what services were offered? Please select all that apply.	Pct%
Credit freeze services	9%
Credit report monitoring services	80%
Fraud alert services	5%
A copy of your credit report from one or more credit bureaus	2%
Identity theft insurance	3%
Identity recovery services (if your identity is stolen)	5%
Other	17%
Total	121%

Q13c. If no, what services would have been most helpful to you? Please select all that apply.	Pct%
Credit freeze services	37%
Credit report monitoring services	52%
Fraud alert services	49%
A copy of your credit report from one or more credit bureaus	5%
Identity theft insurance	46%
Identity recovery services (if your identity is stolen)	23%
Other (please specify)	9%
Total	221%

Q14a. Did you take advantage of these services?	Pct%
Yes	47%
No	53%
Total	100%

Q14b. If you didn't take advantage of these services, why didn't you? Please select only one.	Pct%
I don't believe these services are necessary or helpful	11%
Enrolling myself in these services was too difficult or inconvenient	9%
The services required too much personal information	7%
The services required a co-paid amount	16%
I did not respond to the offer within the required time period	29%
I already subscribe to these services	26%
Other (please specify)	2%
Total	100%

Q14c. If yes, what services did you select? Please select all that apply.	Pct%
Credit freeze services	9%
Credit report monitoring services	86%
Fraud alert services	10%
A copy of your credit report from one or more credit bureaus	8%
Identity theft insurance	5%
Identity recovery services (if your identity is stolen)	1%
Other (please specify)	2%
Total	121%

Q14d. Was your concern or worry about the data breach reduced after using any of these services?	Pct%
Yes	51%
No	49%
Total	100%

Q14e. For each item selected above, please rate the quality of the services you received using the following scale: 1=excellent, 2 = very good, 3 = good, 4 = fair and 5 = poor, 9 = not applicable:	1	2	3	4	5	9
Credit freeze services	2%	1%	4%	0%	0%	92%
Credit report monitoring services	10%	22%	46%	4%	2%	16%
Fraud alert services	3%	6%	0%	0%	1%	90%
A copy of your credit report from one or more credit bureaus	0%	1%	7%	1%	1%	91%
Identity theft insurance	4%	0%	1%	0%	0%	95%
Identity recovery services (if your identity is stolen)	1%	0%	0%	0%	0%	99%
Other	0%	0%	2%	0%	0%	98%
Total	3%	4%	9%	1%	1%	83%

Q14e. For each item selected above, please rate the quality of the services you received using the following scale: 1=excellent, 2 = very good, 3 = good, 4 = fair and 5 = poor, 9 = not applicable:	1	2	3	4	5	Total
Credit freeze services	30%	15%	49%	4%	2%	100%
Credit report monitoring services	12%	26%	55%	5%	2%	100%
Fraud alert services	26%	63%	1%	2%	7%	100%
A copy of your credit report from one or more credit bureaus	4%	7%	70%	10%	8%	100%
Identity theft insurance	74%	1%	24%	0%	1%	100%
Identity recovery services (if your identity is stolen)	100%	0%	0%	0%	0%	100%
Other	0%	0%	100%	0%	0%	100%
Average	35%	16%	43%	3%	3%	100%

If you have questions or comments about this research report or you would like to obtain additional copies of the document (including permission to quote from or reuse this report), please contact us by letter, phone call or e-mail:

Ponemon Institute LLC
 Attn: Research Department
 2308 US 31 North
 Traverse City, Michigan 49686
 1.800.887.3118
research@ponemon.org

Ponemon Institute LLC

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.

ID Experts

www.idexpertscorp.com

ID Experts' mission is to protect Americans from identity theft. For over five years, our identity theft protection experts have helped thousands of victims and we have developed and apply best practices to protect millions of Americans today from this growing problem. We also are trusted by some of America's largest corporations, government agencies and universities to provide them with complete, tailored data breach planning and response services. Our team of experts is passionate about providing personal, fully-managed services to help the largest of organizations as well as individuals and families.

To learn more about ID Experts, visit us on the web at www.idexpertscorp.com, call us at (503) 726-4500 or email request_info@idexpertscorp.com.