Sponsored by the global law firm of

WHITE & CASE LLP

Independently conducted by

National Survey on Data Security Breach Notification

Report September 26, 2005

WHITE & CASE LLP

Ponemon Institute LLC

National Survey on Data Security Breach Notification

Confidential Report Prepared by Dr. Larry Ponemon, September 26, 2005

Recipients of Data Security Breach Notices Are Not Satisfied with Initial Communications

The research is sponsored by the global law firm of White & Case, LLP.

We are pleased to report the results of its National Survey on Data Security Breach Notification. Survey fieldwork was completed on August 25, 2005. This perception-capture research was independently conducted to learn how individuals react to data security breach notifications sent by business, non-profit or governmental organizations as required by new laws. The purpose of this study is to learn how organizations met their legal obligation to notify individuals after the loss or theft of personal information. In addition, this study seeks to understand how individuals reacted to the organization's communication and handling of this critical event.

Invitations to 51,433 adult-aged individuals throughout the United States were sent by e-mail or letter. We received 9,154 usable Web-based survey responses from individuals residing in all major regions, resulting in a 17.8% response rate. Of these respondents, over 11.6% or 1,109 individuals self-reported that they received communications from an organization about the loss or theft of their personal information.

Executive Summary

The National Survey on Data Security Breach Notification addresses the notification practices of U.S.-based organizations in business and government when a data security breach occurs and personal information is either lost or stolen. According to various new state laws and emerging U.S. federal regulations, organizations are required to notify victims of the breach in a timely fashion.

According to our research, individuals receiving the data breach notification tend to blame the organization for not having sufficient controls or safeguards to protect their data. Even if the victims of the breach do no suffer direct negative consequences as identity theft, our research further indicates that they are likely to lose trust and confidence in the organization. Obviously, lost trust will likely cause many customers to churn – especially if they believe the organization's response and handling of the security breach is unsatisfactory to them.

All organizations are vulnerable to a data security breach. However, it seems that what determines an organization's ability to protect its reputation and maintain the trust of its customers and employees in the aftermath of a breach is the quality of the notification. For this reason, we have surveyed individuals who have been notified about a data security breach and asked them specific questions about the content and the process of the notification. The following findings are the most informative about our respondents' perceptions.

General findings – Data breach incidents appear to be a pervasive problem in the United States, becoming more transparent as a result of several new state privacy laws.

- Our study suggests that over 23 million U.S. adult-aged residents recall receiving a breach notification. Approximately 11.6% of survey respondents reported that they have received notification of a data security breach within the last year.
- About 86% of security breaches involved the loss or theft of customer or consumer information. About 14% involved employee, student, medical, and taxpayer data.
- The most likely organizations to report a breach are banks, credit card companies, governmental organizations (including state universities), and health care providers.

- The most common form of communication includes form letters, telephone calls and personalized letters.
- Only 22% of respondents understand what encryption is. Of these individuals, only 5% said the organization reporting the breach had used encryption to protect personal data. The 78% of respondents who know what encryption is reported that the organization still needs to notify victims even if it used encryption technologies.

Communication experience – A majority of respondents are not satisfied with the quality of the notification and communication process.

- The most effective communication method appears to be a combined approach of telephone and letter.
- Over 39% of respondents initially thought the notice was junk mail, spam or a telemarketing phone call. About 51% initially considered the communication an important piece of information.
- About 48% of respondents said that the notice was not easy to understand, and over 49% of respondents believed that the notice did not provide enough details. Respondents want to know more about the protections to be provided by the organization as well as what consequences they could expect. More than 28% of respondents said they had no idea about the facts of the incident even after receiving notification of the breach.
- Only 12% of respondents believed that the breach was communicated within two weeks of the incident. About 19% believe that the data breach was communicated within one month of the incident. Over 32% of respondents do not know the timeframe of the breach.
- Despite negative impressions, about 61% of respondents believed that the message contained in the notice was honest and believable.
- About 46% of organizations offered some form of support or assistance to respondents. The most common type of support provided by organizations included the issuance of new accounts (and credit cards) and closer monitoring of accounts for suspicious activities. About 36% of respondents who requested support did not find the assistance helpful.
- Over 44% of organizations provided telephone contact or a help line for individuals requesting more information about the incident. Over 48% of individuals contacting the organization believed that the organization's responsiveness was good or excellent. The remaining 52% of subjects believed that the organization's responsiveness was poor or fair.

Potential consequences – People are fearful that the data breach will have a significant negative impact on them and their families. As a result, many notice recipients have lost trust and discontinued support for organizations reporting the incident.

- Over 58% of respondents believed that the breach decreased their sense of trust and confidence in the organization reporting the incident. And, over 86% of subjects are concerned or very concerned about how data breach incident will affect them.
- Only 8% of respondents did not blame the organization that reported the breach. Over 40% of individuals said that they might discontinue their relationship, and another 19% have already discontinued their relationship, as a result of the data breach.
- Companies that report a breach to consumers are more than four times (417%) more likely to experience customer churn if they **fail** to communicate to the victim in a clear, consistent and timely fashion.
- Companies that deploy e-mails or form letters to communicate a breach of consumer data are more than three times (326%) more likely to experience customer churn than companies that use telephone or personalized letters (or a combination of both).

Implications for the future – It is not clear whether current notification regulations are perceived as "beneficial" to consumers. A majority of respondents do not have confidence that more stringent regulations will be helpful.

- Over 82% of respondents believed that it is always necessary for an organization to report a breach even if the lost or stolen data was encrypted, or there was no criminal intent. The type of information involved in the breach was also not a factor.
- About 59% of respondents do not have confidence in U.S. state or federal regulations to protect the public from data security breaches by organizations.

Survey

As part of the survey instrument review process, we sought input from a number of learned sources including privacy, data security and regulatory experts.

The survey utilized a fixed cluster sampling frame. The target respondents were recruited based on self-reported demographic criteria matched against national census data. Individuals were invited to participate by e-mail and letter (post card).

Respondents were given the following basic instructions before starting the survey process.

Dear Participant,

Have you recently received a notification from a business, non-profit or governmental organization concerning a data security breach that resulted in the loss of your personal information? If you did, we would like to learn how well you believe the organization communicated the breach to you, and if you are satisfied with the actions it took following the incident.

Please assume that when we refer to "organization" it means the business, non-profit or governmental entity that is reporting the data security breach to you.

We greatly appreciate your response to all survey questions. Please be assured that we will not collect any personally identifiable information. If you have any questions, contact Ponemon Institute at research@ponemon.org or call us at 1.800.887.3118.

Thank you in advance for your participation.

Items on the survey form were randomized or rotated to mitigate order effects. All completed returns were evaluated for consistency and internal reliability before including in our final sample.

Sample

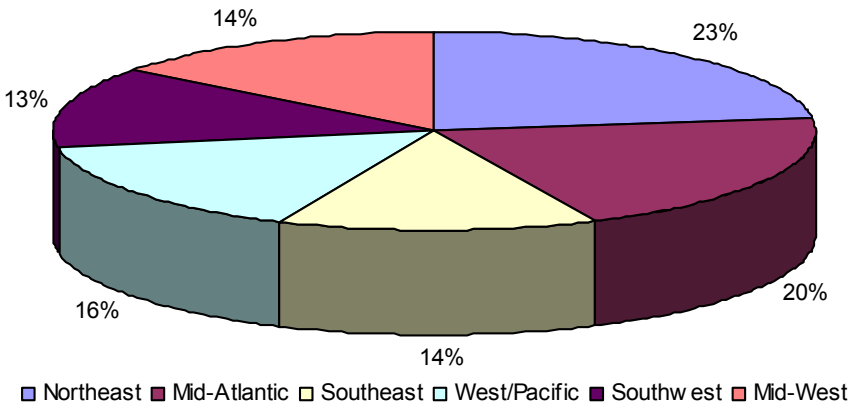
Following are the response statistics and geographic distribution across regions within the United States. In total, 9,525 adult-aged respondents submitted survey results. Of these responses, 371 were removed for inconsistencies. The final sample of 9,154 represents over 17.8% of the sampling frame. Non-response bias was tested and there does not appear to be significant sampling anomalies.

Tables 1a and 1b and the accompanying Pie Chart 1 show that the two most heavily represented regions include the Northeast and Mid-Atlantic regions of the United States.

Table 1a: Sample Characteristics	Total	Pct %
Sample frame	51,433	100.0%
Total responses	9,525	18.5%
Total rejections	371	0.7%
Net responses	9,154	17.8%
Subjects who received notice	1,109	11.6%

Table 1b: U.S. Regions	Freq	Pct%
Northeast	254	23%
Mid-Atlantic	225	20%
Southeast	150	14%
West/Pacific	173	16%
Southwest	148	13%
Mid-West	159	14%

Pie Chart 1: Sample of Respondents Receiving Notice of a Data Breach
by U.S. Geographic Region



Our sample includes U.S. residents who are 18 years or older. Since this research asked respondents to complete a survey on our extranet Web site, most respondents owned or had control over their own computer (desktop or laptop). Subjects were paid a nominal incentive for completing the survey within a pre-defined holdout period. All responses were completed within a 5 week period.

Extrapolation

An objective of our study was to understand the magnitude of security breach notification in the U.S. At the time of this research, 18 U.S. states require some form of notification. Many of these state laws resemble California's SB 1386 that became effective on July 1, 2003.

As noted in Table 2, our sampling procedure suggests that, on average, 11.6% of the general adult aged population received some form of notice. According to a recent press release (dated PR Newswire September 6, 2005), the Identity Theft Resource Center (ITRC) reports that 104 security breaches affecting more than 56.2 million individuals were notified since January 1. We extrapolate that more than 23 million people in the United States already received some form of notification. This population estimate is substantially less than the ITRC number. This may be due to the fact that people who were sent notification ignored the communication, or they received more than one notification. This is suggested by findings reported in Table 6.

Table 2. Extrapolation to the United States Population	Population Estimates
Conservative estimate for U.S. residents, 18 years and older	198,431,000
Percentage from sample who recall receiving a notice	11.6%
Estimated U.S. population of adults receiving notice	23,103,410
Estimated number of notifications sent (based on ITRC report)	56,200,000
Difference between sample and media estimates	33,096,590
Percentage difference	59%

Detailed Findings

The actual survey frequencies and percentage frequencies are reported in tabular format. Following is a control question asked all respondents. Pct% means that the tabled percentages sums to the sample total. Tot% means that the table percentages sum to the response total (which is greater than the sample total if the question requested more than one response).

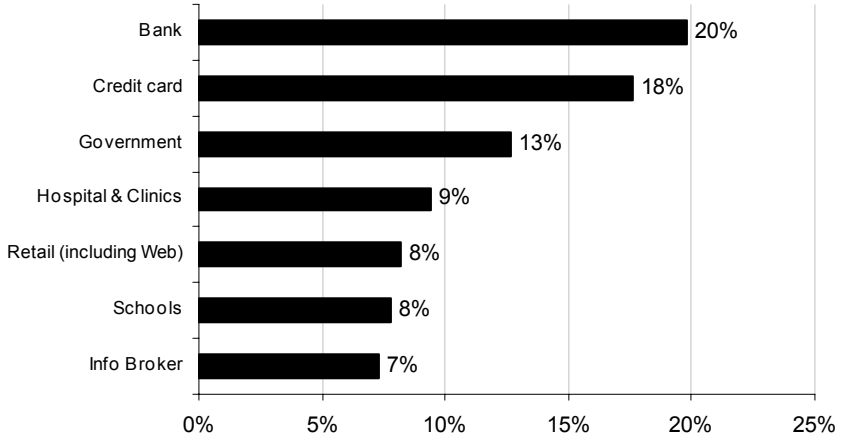
Table 3. Has any organization ever notified you about a data security breach that involved your personal information?	Freq.	Pct%
Yes	1,109	12%
No	6,289	69%
Unsure/don't recall	1,756	19%
Total	9,154	100%

The remainder of the analysis focuses on the 1,109 respondents who self-reported that they received notification of a data security breach. Table 4 shows that 86% of data breaches involved the loss or theft of customer or consumer information.

Table 4. Please indicate the type of personal information that was involved in this data security breach?	Freq.	Pct%
My employee records	113	10%
My customer or consumer information	955	86%
Other personal information	41	4%
Total	1,109	100%

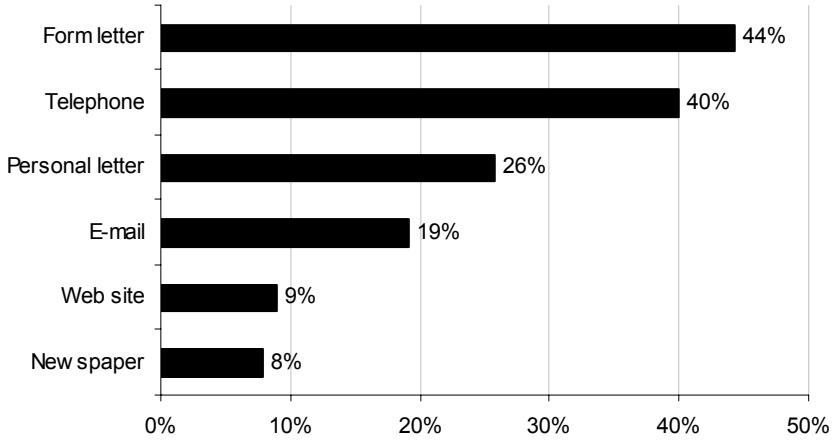
Bar Chart 1 reports the organizational types that reported the breach. The findings show that banks (20%), credit cards (18%), government entities including state universities (13%), and health care providers (9%) were the most likely organizations to provide notice.

Bar Chart 1: Types of Organizations Reporting the Data Security Breach



The next bar chart shows that form letters (44%), telephone calls (40%) and personal letters (26%) are the most frequently used communication channels for notifying individuals.

Bar Chart 2: Communication Channels Deployed for Notification



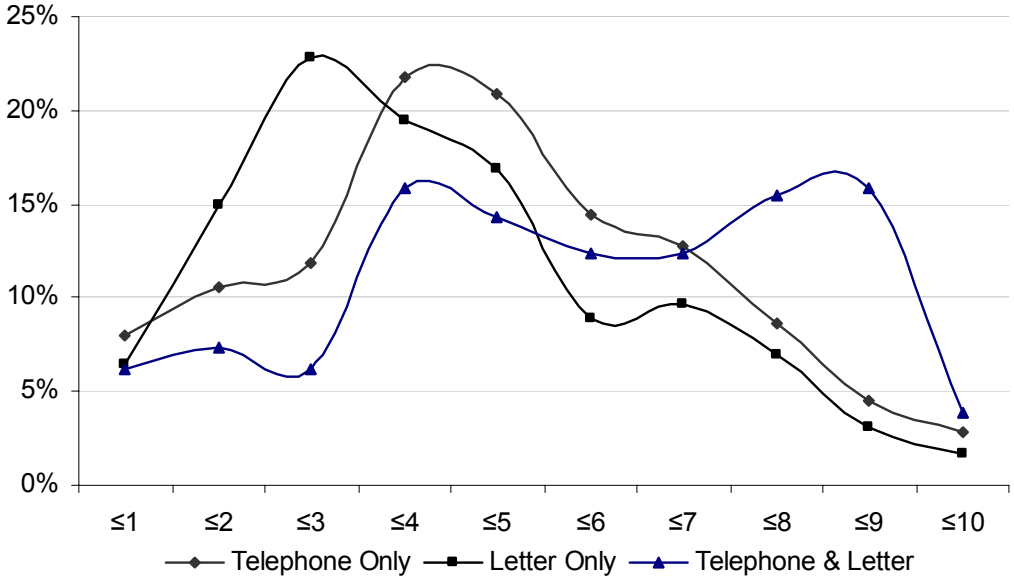
The following line graph reports a pattern of results based on individual responses to an adjective scale provided in the survey instrument, defined as follows:

I believe that the organization did a good job in communicating and handling the data security breach.

Agree|_____|_____|Disagree

Results are organized from lowest (disagree=1) to highest (agree=10) in terms of respondents' perceived effectiveness of the organization in managing the breach incident.

Line Chart 1: Perceived Effectiveness in the Communication and Handling of the Data Security Breach Incident by Communication Methods



The line chart provided above is organized into three curves by communication channel, as follows: (1) telephone, (2) letter, and the (3) combination of telephone and letter. The skewed distributions suggest that a majority of respondents hold negative perceptions. As shown, telephone earns more favorable opinions than letter. Telephone and letter combined earns the most favorable ratings from respondents.

Table 5a shows that almost half of respondents (49%) do not believe that the organization provided enough details about the breach event.

Table 5a. Did the notice provide enough details about the data security breach?	Freq.	Pct%
Yes	567	51%
No	540	49%
Total	1107	100%

For those stating that they did not get sufficient details, Table 5b, shows the facts that were most likely missing from the report. The two top issues are: (1) the protections to be provided by the organization reporting the breach (50%) and (2) the expected consequences of the breach (40%).

Table 5b. If you answered no, what facts were missing that was important to know about? Please select top two choices only.	Freq.	Tot%
The personal data that was actually stolen.	115	21%
The individuals or third parties who wrongly acquired my information.	86	16%
The expected consequences of the breach to me and my family.	214	40%
The date the breach most likely occurred,	150	28%
The criminal investigations that are being conducted to identify those responsible for the breach.	78	14%
The protections the organization will provide to minimize the harm to me and my family.	269	50%
The steps the organization is taking to prevent future security breaches.	57	11%
Other (please explain)	52	10%
Total	1021	

Bar Chart 3 reports the degree of concern that respondents experienced after receiving notice of the breach. As shown, over 86% of individuals were either concerned or very concerned after learning about this incident.

Bar Chart 3: How Concerned Were You After Receiving Notice?

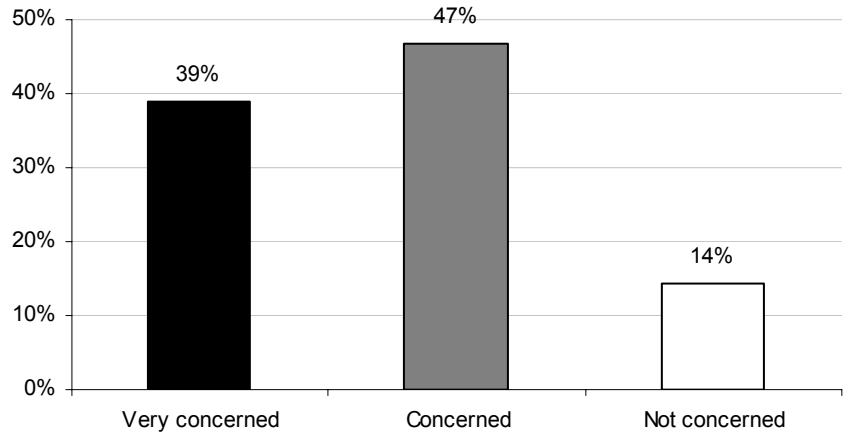


Table 6 reports the respondents' initial reaction to the notification. It is interesting to note that over 39% of respondents thought the initial communication was either junk mail, spam or a telemarketing phone call.

Table 6. What was your initial reaction to the data security breach notification (sent by either by mail, e-mail or telephone)?	Freq.	Pct%
At first, I thought the letter was junk mail.	162	15%
At first, I thought the e-mail was spam (or a phishing attack).	94	8%
At first, I thought the call was from a telemarketer.	175	16%
I knew that this was an important communication.	565	51%
I do not remember my initial reaction to the communication.	112	10%
Total	1108	100%

Bar Chart 4 shows how individuals respond to the organization reporting the breach. Only 8% of respondents do not assign blame to the organization reporting the breach. Over 40% of respondents said that they might discontinue their relationship, and another 19% have already discontinued their relationship, as a result of the breach.

Bar Chart 4: Respondents' Reactions to the Notice

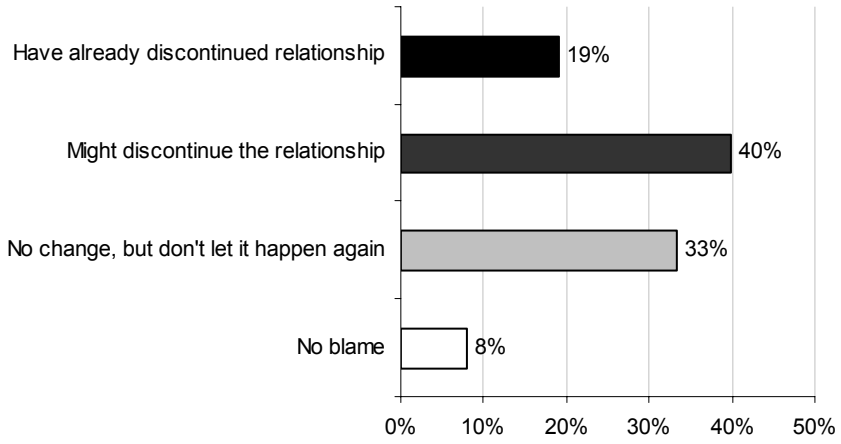


Table 7 reports what respondents know about the data breach incident. It is interesting to note that about 28% of individuals said that they have no idea about what the incident is even after receiving notification.

Table 7. What do you know about the data breach incident?	Freq.	Pct%
My data was most likely stolen.	413	37%
My data was most likely lost or misplaced by the company.	200	18%
My data was most likely shared with third parties without my permission.	132	12%
I have no idea what the data breach incident is about.	305	28%
Other (please explain)	56	5%
Total	1106	100%

The next bar chart reports the types of data involved in the breach. It shows that the most likely data elements involved in the breach include: name (54%), account numbers (41%), Social Security numbers (38%), and credit card numbers (37%).

Bar Chart 5: Types of Data Involved in Breach

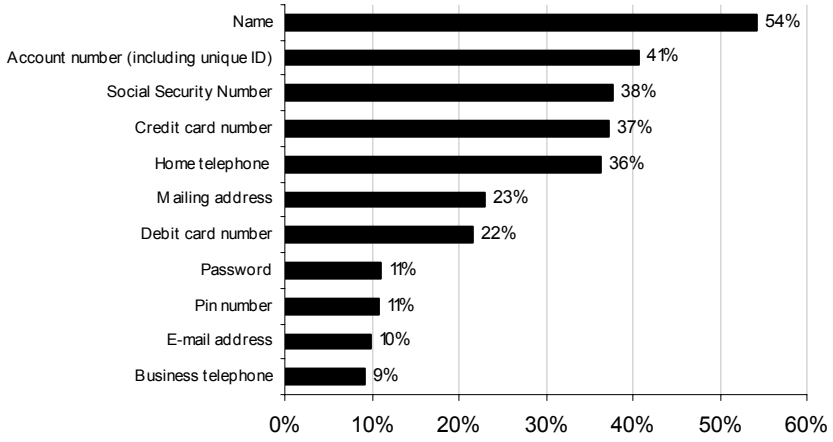


Table 8 reports the respondents' understanding about encryption and how it affects the organization's reporting obligations. As shown, only 22% know what encryption is.

Table 8a. Do you know what encryption is?	Freq.	Pct%
Yes	243	22%
No	864	78%
Total	1107	100%

Only 5% said that the organization communicated to them that encryption was used to protect personal data.

Table 8b. If you answered yes, do you know if the organization reporting the breach used encryption to protect your personal information?	Freq.	Pct%
Yes	12	5%
No	43	18%
Unsure	188	77%
Total	243	100%

About 78% of respondents who know what encryption is said that the organization should still report the breach incident, even if the lost or stolen data was encrypted.

Table 8c. If you answered yes, assuming that your lost or stolen data was encrypted, do you think that it is still necessary for the organization needs to report this data breach to you?	Freq.	Pct%
Yes	189	78%
No	32	13%
Unsure	21	9%
Total	242	100%

As shown in Table 9, 52% respondents said that the notice was not easy to understand.

Table 9. Was the notice easy to understand?	Freq.	Pct%
Yes	529	48%
No	578	52%
Total	1107	100%

Table 10 shows that the most important improvements to the notice include (1) disclose all facts, (2) explain risks and harms, and (3) don't "sugar coat" the message.

Table 10. What could the organization do to improve the communication? Please check the top two choices only.	Freq.	Tot%
Reduce technical or legal terms.	199	18%
Do not "sugar coat" the message.	379	34%
Make the communication more personal.	304	27%
Disclose all facts.	458	41%
Explain the risks or harms that I will most likely experience as a result of the breach.	403	36%
Make the font or type size larger.	85	8%
The notification should be in the native language of the victim.	83	7%
Nothing could be done to improve the message	83	7%
Other (please explain)	48	4%
Total	2042	

Bar Chart 6 shows the length of time it took the organization to notify victims after the breach event. Over 32% of respondents could not respond because it was not included in the notice document. Only 12% of subjects received notification immediately or within the first two weeks.

Bar Chart 6: How Long After the Breach Did You Receive Notice?

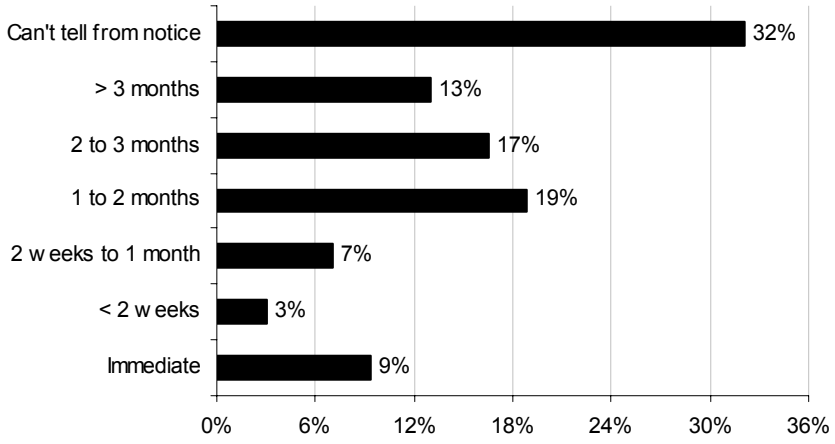


Table 11 reports whether or not the organization provided a telephone contact point or help line for those individuals interested in learning more about the breach event. As shown, 44% of respondents said that the organization did provide a telephone support line.

Table 11a. Were you given telephone contact information in case you wanted to talk to someone about your concerns?	Freq.	Pct%
Yes	484	44%
No	410	37%
Don't recall/unsure	212	19%
Total	1106	100%

Over 41% of respondents said that they actually called the number provided.

Table 11b. If you answered yes, did you call the organization?	Freq.	Pct%
Yes	199	41%
No	283	59%
Total	482	100%

About 48% reported that the organization's responsiveness to the call was either good or excellent.

Table 11c. If you answered yes, how would you rate the company's responsiveness to your call?	Freq.	Pct%
Excellent	41	21%
Good	54	27%
Fair	71	36%
Poor	33	17%
Total	199	100%

Table 12 reports that 61% of the respondents believe that the organization's message was honest and believable.

Table 12. In your opinion, was the message conveyed by the organization about the data security breach honest and believable?	Freq.	Pct%
Yes	679	61%
No	428	39%
Total	1107	100%

The following bar chart shows that, despite the believability of the message, 58% of respondents said that the breach event has diminished their trust and confidence in the organization. It is interesting to note that 12% of respondents reported that the incident actually increased their trust in the notifying organization.

Bar Chart 7: How Has the Breach Incident Affected Your Trust and Confidence in the Organization?

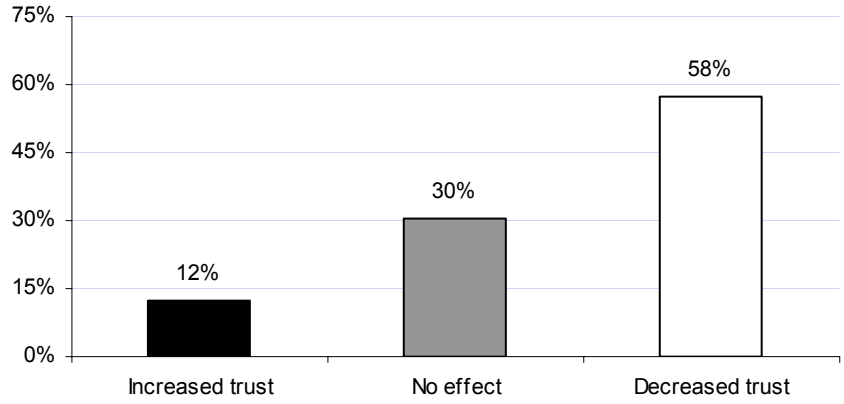


Table 13 reports the organization's support provided to breach victims. As shown, 46% said that the organization offered some form of assistance. About 9% can't recall whether or not the organization offered support or assistance to them.

Table 13a. Did the organization offer to help you?	Freq.	Pct%
Yes	508	46%
No	502	45%
Can't recall	99	9%
Total	1109	100%

The following table shows that 90% provided a new account (or issued new credit card), and 75% of organizations provided close monitoring for suspicious activities.

Table 13b. If you answered yes, what support or assistance did the organization provide? Please check all that apply.	Freq.	Tot%
Counseling on how to protect me and my family's identity.	144	28%
Free or discounted access to credit report monitoring services.	131	26%
Closer monitoring of the organization's accounts to flag any suspicious activities.	379	75%
Issuance of new account or credit cards.	458	90%
Free computer security software.	32	6%
Other (please explain)	56	11%
Total	1200	

Over 36% of respondents said that the support was either helpful or very helpful. About 64% believed that the support was either adequate or not helpful.

Table 13c. If you answered yes, how would you rate the organization's help?	Freq.	Pct%
Very helpful	49	10%
Helpful	134	26%
Adequate	188	37%
Not helpful	135	27%
Total	506	100%

Table 14 reports the harms experienced by respondents. About 31% said that they have not been harmed by the breach. Sixty-one percent said that they experienced additional worries or concerns, and 56% said that they spent time resolving potential problems that resulted from the breach. Less then 3% said that their identity had been stolen.

Table 14. Have you been harmed by this data security breach? Please check all that apply.	Freq.	Tot%
I have had no problems.	344	31%
I am more worried about the security of my personal information.	678	61%
My identity has been stolen.	33	3%
Marketers have violated my privacy.	240	22%
I have had to spend time resolving problems as a result of the breach.	616	56%
Other (please explain)	45	4%
Total	1956	

Table 15 shows 82% of respondents believed it is **always** necessary for an organization to report a breach without consideration for encryption, nature of leaked information, or criminal intent.

Table 15. When is it not necessary for an organization to report a data security breach to you? Please check all that apply.	Freq.	Tot%
When my personal data is encrypted.	32	3%
When the data stolen is only my name and address.	154	14%
As long as my Social Security number or credit card information are not stolen.	114	10%
When the breach occurred as a result of an employee error and there was no criminal intent.	133	12%
None of the above	904	82%
Total	1337	

Bar Chart 8 shows that over 59% of respondents do not have a high degree of confidence that U.S. state or federal regulations are adequately protecting the public from data security breaches by business, non-profits and governmental organizations.

Bar Chart 8: Confidence in U.S. State and Federal Regulations to Protect Privacy and Data Security?

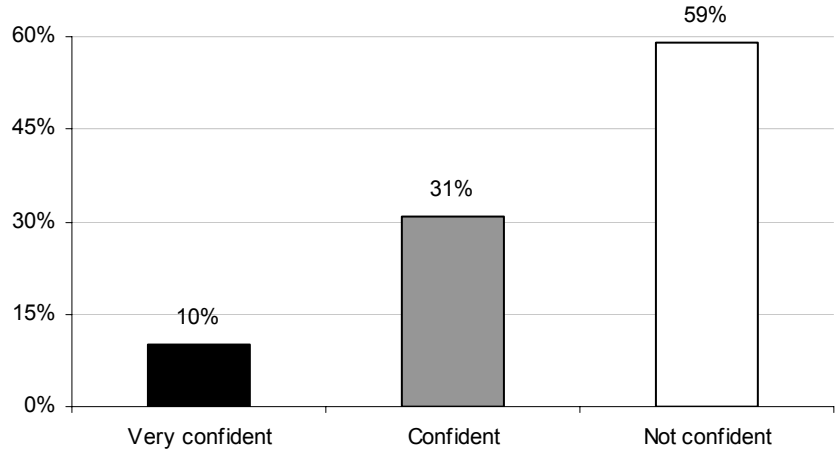


Table 16 reports the steps respondents are taking to minimize harm or threats caused by the data breach incident, such as identity theft. Exactly half (50%) of the respondents state they are doing nothing new to protect themselves. About 21% say they are monitoring their credit reports more closely, and 9% state that they bought crediting monitoring services. About 5% say that they hired an attorney for possible legal action.

Table 16. What are you doing to protect yourself from identity theft? Please check all that apply.	Freq.	Tot%
Nothing	553	50%
Cancelled all credit or debit card account affected by the breach.	508	46%
Cancelled bank accounts affected by the breach.	132	12%
I will monitor my credit reports.	233	21%
I hired a paid service to monitor my credit reports.	103	9%
I hired a lawyer to file lawsuit against the organization.	54	5%
Total	1583	

Protecting Reputation

Table 17 reports that 58% of respondents believed that their overall sense of trust and confidence in the organization reporting a breach has been diminished. Clearly, these findings can seriously affect the organization's economic condition in terms of decreased loyalty and increased churn.

Table 17. How did this incident change your trust and confidence in the organization?	Freq.	Pct%
Increased my trust and confidence in the organization.	135	12%
Had no effect on my trust and confidence in the organization.	334	30%
Decreased my trust and confidence in the organization.	635	58%
Total	1104	100%

We attempted to better understand why 42% of respondents felt that their trust or confidence in the reporting organization was not affected by the breach incident. The following table reports a summary of key findings for these 469 individuals (135 + 334), which we call the "positive group" in this analysis.

Table 18. Attributes of Effective Data Breach Notification	Freq. Positive Group	Pct%	Overall Sample	Difference
Total sub-sample (Table 16 135 + 334 = 469)	469	42%		
First reaction, viewed communication as important	362	77%	51%	26%
Organization provided additional support	319	68%	46%	22%
Organization provided telephone helpline	295	63%	44%	19%
Notice provided enough details	318	68%	51%	17%
Contact made by telephone and letter	186	40%	23%	16%
Received notice within one month of incident	162	35%	19%	15%

The difference – computed for six attributes discussed in the previous section – is defined as the percentage for the entire sample minus the percentage for the positive group. Our results show that clarity of the notice, channels of communication, availability of support, and timeliness of the report are all important to preserving the victim's trust and confidence in the organization that is reporting the data breach.

As shown, 77% of the positive group knew that the communication was important when they first received it, as compared to only 51% for the entire sample. About 68% of respondents in the positive group were offered some form of support or assistance by the reporting organization, as compared to 46% for the full sample. Sixty-three percent of the positive group was given access to a telephone helpline, as compared to 51% of the sample. About 40% of the positive group was notified about the breach by both telephone and letter, as compared to only 23% of the entire sample. Finally, respondents in the positive group were more likely to receive initial notice about the breach within one month following the incident (35% versus 19%).

Preventing Churn

We also looked at the likelihood of a data breach causing customers to terminate their relationship with the organization. According to our study, the loss of trust among customers can be so significant that following a breach they may decide to take their business to another company.

Table 19. What statement best describes your reaction to the organization reporting the breach?	Freq.	Pct%
The organization reporting the breach is not to blame.	88	8%
I will continue my relationship with the organization as long as it does not happen again.	368	33%
I might discontinue my relationship with the organization.	441	40%
I will (or have) discontinue(d) my relation with the organization.	210	19%
Total	1107	100%

As shown in Table 19, 41% or 456 or the study's respondents reported that they will not terminate their relationship as a result of the breach (this is defined as our no churn subgroup). About 19%,

or 210 respondents, reported that they plan to terminate or have already terminated their relationship as a result of the breach incident (this is defined as the churn subgroup).

We were interested to learn what factors contained within our survey instrument contributed to the respondent's decision to churn. To perform this analysis, we used a nonlinear (logit) regression analysis technique for two subgroups defined above as churn and no churn. As shown in Table 20, the analysis revealed some interesting findings.

Table 20. Importance of clarity, timeliness and believability of message contained in the notice and probability of churn intention.	Churn	No Churn
Observations in analysis	210	456
Notice provided enough details	No	Yes
Received notice within one month of incident	No	Yes
Message conveyed was honest or believable	No	Yes
Probability of Churn	37.9%	9.1%

For respondents who stated that the notice did not provide enough detail, was not timely, and was not believable, the probability of churn is 37.9%. In contrast, respondents who stated that the notice provided enough details, was timely and was believable, the probability of churn is 9.1%. Clearly, this difference in the decision to churn is very significant. While many other unexplained factors might result in a loss of customers, our analysis suggests that if an organization's notice is negatively received, the probability of churn is likely to be more than four times (417%) higher than if the notice is positively received.

Using the same regression technique, we were interested in learning how communication methods or channel affected the individual's churn intention.

Table 21. Communication methods deployed and the probability of churn intention.	Churn	No Churn
Form letter	Yes	No
E-mail	Yes	No
Personalized letter	No	Yes
Telephone contact	No	Yes
Probability of Churn	28.1%	8.6%

Table 21 shows that for companies communicating the data breach by e-mail or form letter, the probability of churn is 28.1%. In contrast, companies that used personalized letters or outbound telephone contact to notify individuals about the breach, the probability of churn decreases to 8.6%. This result suggests that the likelihood of churn is over three times (326%) higher for companies that use e-mails or forms to communicate the breach than for companies using personalized letters or telephone calls. Again, many other factors may explain the significant variance in these results.

Demographic Questions

Following are the demographics collected from all survey respondents in this national study. Please note that additional analysis has been conducted to determine if certain demographic variables are correlated to the survey responses.

Respondent's age range	Freq.	Pct%
Age 18 to 25	202	18%
Age 26 to 35	270	24%
Age 36 to 45	249	23%
Age 46 to 55	166	15%
Age 56 to 65	125	11%
Age 66 to 75	68	6%
Age > 75	26	2%
Total	1106	100%

Income range	Freq.	Pct%
Income < 20k	47	4%
Income 20k to 40k	144	13%
Income 41k to 60k	343	31%
Income 61k to 80k	287	26%
Income 81k to 100k	145	13%
Income 101k to 150k	54	5%
Income 151k to 200k	43	4%
Income > 200k	42	4%
Total	1105	100%

Highest level of education	Freq.	Pct%
High School	257	23%
Vocational	201	18%
College (4 yr)	456	41%
Post Graduate	141	13%
Doctorate	51	5%
Average	1106	100%

Gender	Freq.	Pct%
Female	565	51%
Male	543	49%
Total	1108	100%

WHITE & CASE LLP

Ponemon Institute LLC

About the study's sponsor

White & Case LLP is a leading global law firm with nearly 1,900 lawyers in 38 offices in 25 countries. Our clients value both the breadth of our network and depth of our US, English and local law capabilities in each of our offices and rely on us for their complex cross-border commercial and financial transactions and for international arbitration and litigation. Whether in established or emerging markets, the hallmark of White & Case is our complete dedication to the business priorities and legal needs of our clients.

White & Case's Privacy Practice operates at the forefront of privacy issues and data protection laws. We advise clients on how to adopt sound privacy practices, avoid privacy risks, and protect their competitive advantage. We also represent clients in privacy-related litigations. Each year we host an annual symposium, regularly write articles, publish or sponsor surveys related to complex privacy issues. For more details, visit www.whitecase.com or contact David Bender, co-head, White & Case LLP Privacy Practice, at 1-(212) 819-649 or via email at dbender@whitecase.com.

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.

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 or reuse this report), please contact by letter, phone call or email:

Ponemon Institute, LLC
Attn: Research Department
212 River Street
Elk Rapids, Michigan 49629
1.800.887.3118
research@ponemon.org