Abstract

Organizations are exposing personal information at an alarming rate, with a probable correlation to an increase in identity theft victims. Data breaches are a growing threat to commerce, concern for policymakers, and businesses; as well as a hotly debated topic among legislators and academics.

This project offers a unique perspective on this topic since the researcher has visibility into dozens of organizations and hundreds of data breach events. This two part research project will clarify important points, and expose fundamental research gaps that exist today.

Key results suggest that the phenomenon known as “over-notification” does not truly exist, that individuals are not overly anxious upon receipt of notification letters, and that additional research is needed in a few key areas regarding the content of notification letters.

Into the Breach: Lessons Learned from Data Breach Research

By

Christine Arevalo

A Professional Project Submitted to the Faculty of

Utica College

January 1, 2010

In Partial Fulfillment of the Requirements for the Degree

Master of Science in Economic Crime Management

Table of Contents

Table of Figures

Index of Tables

Index of Appendices

Acknowledgements

I cannot thank enough all of my friends and colleagues at ID Experts nor the ID Experts members who participated in this blind survey. Thank you for being there for me, and for the time and talent you have shared with me. You have all been generous with your expertise and contributions in at least a million ways. I couldn't go without naming Chris Kane who has been a champion and a positive influence since the day I met him.

Thank you to the industry thought leaders who have inspired me, as well as motivated me and given me unique opportunities to study in this space. Jim McCabe of ANSI, Dr. Larry Ponemon, James Van Dyke of Javelin Strategy and Research, and Rick Kam; to name a few.

Thank you to my family who has stood behind me on this journey from the very start. Your confidence when I seriously needed it will not be forgotten. The same can be said for Cohort 16 – who I spoke to more than my own family at times. I'm not sure if you needed me, but I certainly needed you.

My appreciation also extends to the faculty and alumni of Utica College, in particular Adjunct Professor R. A. (Andy) Wilson; you have been so unselfish with your time and helped me with such dedication and prose. Words cannot express my gratitude to what you have contributed to my success as a student and to this project. And the Alumni, *you know who you are*, you gifted me inspiration and support, particularly when I was lost.

Finally, to my academic review board, Rick Kam, Adjunct Professor Vernon McCandlish, and Adjunct Professor R. A. (Andy) Wilson, thank you for your critiques, for your time, and for pushing this project past the finish line.

I couldn't have done this without all of you.

INTRODUCTION

In 2009 there were 498 data breaches in the U.S., affecting 222,477,043 individuals (Identity Theft Resource Center, 2010a). As alarming as these figures sound, they may well be underreported, since these figures represent only events made public presumably because of statutory requirements, through data breach notification letters, the Freedom of Information Act 5 U.S.C. § 552, Attorneys General websites, and other good faith communications from organizations who experienced them. Among the most notable of public data breach events in recent years are those at TJ Maxx (The TJX Companies, Inc.), Heartland Payment Systems (the largest data breach in recorded history with an impressive 134 million records exposed), HSBC, and ChoicePoint.

Data Breaches are Expensive

The lessons learned from examination of these events are plentiful. One aspect that seems to gain the most attention is the costs associated with a data breach event. For the purposes discussed in this paper, a data breach is defined as the intentional or accidental misappropriation of personal information by an entity. The costs to an organization responding to a data breach are staggering: according to research conducted by the Ponemon Institute (founded by Dr. Larry Ponemon in 2002), on average an organization can expect expenditures of upwards of $204 per affected individual. In 2009 the average total cost of a data breach was $6.75 million, up from $6.65 million in 2008 and $6.35 million in 2007 (Ponemon Institute, 2010). In 2009, HSBC experienced a data breach and was fined £3 million ($5 million U.S. Dollars) by the Financial Services Authority, and the company will incur more costs to address the breach itself (Treanor, 2009). ChoicePoint settled lawsuits

relating to their data breach for $15 million and paid another $5 million to help victims affected by the incident (FTC, 2006).

Another example of high breach costs is a very recent data breach of 1.5 million medical records, lost by one of the largest U.S. publicly traded managed health care organizations, Health Net. Connecticut's Attorney General, Richard Blumenthal, is suing Health Net of Connecticut, alleging the company failed to secure patient medical records and financial information prior to the incident, which involved the loss of an unencrypted device (Connecticut Attorney General's Office, 2010). This incident and the consequences of such a massive data breach will affect this organization from a punitive perspective, not only in loss of reputation.

Ramifications and consequences to businesses who report a breach include potential fines from government and other regulatory agencies, lawsuits from affected individuals, bad publicity, and lost customers and employees, all of which can have a devastating impact on revenues, shareholder value, and overall brand image. Some of these costs are more tangible and measurable than others, leaving organizations to determine their actual risk with little empirical evidence to draw upon.

Victim Perceptions and Other Stakeholders

Another aspect of this issue that gains just as much attention as how organizations that lose information deal with the aftermath, is how victims perceive data breach events and subsequently respond to the organizations responsible for them. When an organization loses the personal information of its employees, a hospital loses patient files, or a business loses the data of their customers, a clear trail of uncertainty and outrage is left behind.

There are other major stakeholders in the data breach issue:

Lawmakers. Who seek to address these issues from a policy perspective. They look to implement legislative mandates to help prevent individuals from becoming victims of identity theft, and hold business responsible for the safekeeping of their constituents' personal information.

Academics. Who are researching and publishing more and more research to understand the real impact of lost and stolen data on society, businesses, and from a policy efficacy perspective.

Businesses. Seeking to do the right thing by their customers. They look to adhere to regulatory notification requirements policymakers have put into place while looking at data breach remediation as a business risk.

Individual consumers. The real victim and major stakeholder. Consumers are clearly the most confused of all, and therein lies the dilemma for businesses deciding to notify or not.

With the stakeholders and issue-at-hand outlined, we will continue this examination of the full scope of the problem and the best way to address it.

Statement of Problem

There have been many reports, research projects, white papers, and opinion pieces written on data breaches. What is currently lacking is an analysis of the lessons learned in a manner that accurately identifies commonly presented threats such as lost business, decreased confidence in a business, ill-effects on brand, public perception, lawsuits, and regulatory fines that can all but cripple a company. Another segment of published reports on this topic focuses heavily on mitigation strategies and best practices, such as technological fixes, data loss prevention, policy and procedure, and other solutions aimed at preventing data breaches in the first place.

State and Federal Legislation

There are regulatory requirements for organizations who suffer a data breach. Several years after California enacted The Database Breach Notification Security Act (SB-1386 - Â§ 1798.82) in September 2002, over 45 states, plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands had followed suit and mandated their own security data breach laws. Many of these state guidelines obligate organizations to follow specific notification guidelines and requirements or face severe penalties and sanctions. Federal laws have also followed suit, most notably in the healthcare field with the Health Information Technology for Economic and Clinical Health (HITECH) Act (42 U.S.C 201) and the Health Insurance Portability and Accountability Act (HIPAA) (Public Law 104-191).

Continued legislation has protected consumers' personal information and encouraged education, preparation, and compliance from organizations when faced with a possible breach. These laws are aimed at increasing safeguards for personal information, and encouraging diligence in choosing with whom consumers will do business. Another outcome

of this patchwork of laws is the general requirement for entities suffering a data breach to notify those affected via a communication vehicle we will refer to as a notification letter.

Best Practices

We see best practices constantly emerging in commercial and government sectors. These best practices are typically the result of respected organizations that have established themselves as corporate role-models, setting rigorous standards as they lead others in the mission of protecting valuable personal and propriety information.

Additional sources of best practice concepts come from experts and anti-fraud professionals with training, education, and experience that place them on the front line preventing, detecting, investigating, and resolving data breach issues. Many of these best practice concepts are now part of federal and state law, while other ideas are simply a matter of good common sense.

Finally, life lessons are a source of best practices, from organizations that have failed to institute even basic protections and are exploited in the media as examples of poor corporate partners. Many of these firms have also been the center of regulatory scrutiny and have endured fines as a result. Providence Health and Services is a good example (Health & Human Services, 2008).

The organizations who implement best practice concepts understand the importance of having a plan of action for a data breach response, and how and when to make public notification to customers, along with other important considerations. It is these organizations that will survive a data breach, and increase customer loyalty through their swift and decisive actions.

Conversely, the lack of planning and a poor data breach response will be costly. Often the lack of proper public notification will attract negative attention from the media and government regulators. The financial costs associated with customer churn, lost business, and the legal actions that follow (i.e., civil and class action suits) can rob profit, and cripple or destroy organizations. That said, even when a breach response is seamlessly executed, an organization still faces at least some risk of fines or other related expenses.

Does a Data Breach Equal Identity Theft?

Experts question any direct correlation between data breaches and identity theft, but recent statistics suggest that those affected by a data breach are four times more likely to become an identity theft victim (Javelin, 2009). Experts also debate whether proper notification to an individual whose personal information was compromised via a data breach event helps the individual take necessary precautions to prevent fraudulent activity from occurring. These experts are also trying to understand exactly how individuals who receive data breach notification letters perceive them and potentially react. There are many claims that consumer confidence is shaken by these letters and as a result individuals will take their business elsewhere. A 2008 survey of U.S. consumers found that an average of 79 percent cite loss of trust and confidence in any business they deal with as a consequence of a security or privacy breach (CA, Inc., 2008).

Is it Expensive to Notify or More Expensive Not to Notify?

Many businesses claim that it is cost-prohibitive to notify their customers of a compromise of personal information. Even businesses who do act responsibly and notify their consumers of a breach receive feedback that the customers found the notice letters complicated, hard to understand, and not helpful (Ponemon, 2008). As policymakers

continue the trend toward broad notification laws, domestically and abroad, studying the efficacy of data breach notification requirements will have strategic value to the identity management community.

Judging by the "chatter" in the identity management community, the consensus is that there is very little dependable research to prove data breach impact on businesses bottom line, best response strategies, data breach notification law efficacy, data breach response as a way to enhance consumer perceptions, or any benefits of notification beyond compliance.

All of these areas are in need of further investigation. Many business risk analysts and legal experts have written position papers encouraging certain strategies in response to a breach; but, there is a lot of conflicting information on the subject.

According to the researcher's inventory, no research was identified that answers important questions such as:

- Do consumers even know who has lost their data?
- Are consumers being over-notified?
- Do notice letters help or hinder the individual's ability to protect themselves from fraud? Is there even a correlation between data breaches and identity theft, if so what?
- Does the content of the notice letter affect the consumer perception about the organization that suffered the breach?
- Are consumers being offered products and services intended to protect from the threats of identity theft and are they taking advantage of them?

- Do consumers understand the circumstances that led to their data being lost or stolen?
- Do consumers feel anxious upon receipt of a data breach notification letter?

Limited *published* analysis has been conducted on the economic impact to businesses that suffer a data breach event. What still seems to be missing is research that better defines the financial impact beyond hard costs; answers to questions such as:

- Does effective notification protect the value of the organization's short-term and long-term value (i.e., stock price)?
- Does effective notification require short-term expense but achieve long-term savings?
- Does notification of a data breach cause consumers to change their buying behavior or adversely affect brand loyalty?
- What are the financial and employment impacts on business associates who lose a client's data?

This Research Project Complements Other Work

This applied research project contains two parts. The researcher has reviewed the relevant works of others concerning data breaches in an effort to better quantify the lessons available, identify opportunities, and better prepare an organization's management team to make the right decisions. Then, to complement the work of others, the researcher prepared and dispatched a survey to 536 individuals and has performed a detailed analysis of the responses.

Research Goals and Objectives Have Been Met

The primary purpose of this research was to learn how data breach victims react to notification letters and their subsequent perception of the organization that lost their personal information. The research findings allow the researcher to discuss the phenomenon known as "over-notification" as it relates to the surveyed population. Finally, the researcher examined responses of qualified survey participants to determine how receiving these letters made them "feel" and if receipt of such letter caused them to change the way they do business with the responsible organization.

LITERATURE REVIEW

Calculating the expenses associated with responding to a data breach can be mind-boggling. Arriving at a true number after factoring in costs associated with legal fees, call centers, lost employee productivity, business interruption, regulatory fines, plummeting stocks, and possible customer erosion may be impossible (Kark, Stamp, Penn, & Dill, 2007). Even determining the full scope of the problem as it relates to a true number of exposed individuals has proven challenging for leading organizations.

In 2009 alone, the Identity Theft Resource Center (ITRC) has accounted for more than 222 million potentially compromised records (ITRC, 2010b). The ITRC collects and maintains a list of publically available information about data breaches. Interestingly however, they report that of the more than 52% of the breaches reported, no information was provided as to the number of individuals involved (ITRC, 2010b). The fact this figure may be underreported is assumed, and the full scope of the data elements exposed remains unknown.

According to Gartner, Inc., increasing reports of lost consumer data files and disclosures of unauthorized access to sensitive personal data are taking a toll on consumers' confidence particularly in the Internet commerce arena (Gartner, 2005). Every day we are bombarded with reports about data breaches and the decrease in customer confidence that results when organizations lose personal information. This potential impact to the bottom line is an increasing concern for businesses.

A Javelin Strategy and Research survey reveals that an organization’s reputation has a significantly greater value than any financial loss that the organization may suffer. The survey identified that as a result of a poorly executed data breach response, the scar on a company’s reputation, image, or brand can be detrimental to its relationship with its

customers. “While data breaches can cost tens of millions of dollars to repair because of fines, security upgrades and notification efforts, reputation is one asset that may not be guaranteed as fully restorable” (Javelin, 2008). Today’s economic conditions also exacerbate concerns about brand and reputation since many businesses cannot afford to lose customers as a result of a poorly executed data breach response.

A more recent survey by Javelin based its conclusions on interviews conducted with some 5,000 U.S. adults. Findings included the fact that data breaches continue to be a source of compromised personal identity information, leading to identity theft (Javelin, 2010). Javelin has been surveying the U.S. population on this topic for seven years, and has measured a continuous rise in identity theft related crimes.

In a survey commissioned by ID Experts, consumers were asked to provide a “report card” and rate data breach response, including notification letters. Questions were developed with the objective to better understand consumer perceptions in the wake of frequent data breach notifications, and the questions administered by the Ponemon Institute. Key findings revealed that the majority of notification programs were perceived as ineffective by consumers, resulting in loss of business to the organization involved. Fully 63% of survey participants said the notification letters they received offered no direction on the steps that they as a consumer should take to protect their personal information. As a result, 31% said they terminated their relationship with the organization from where the data breach occurred (Ponemon, 2008).

Leading organizations, the Better Business Bureau (BBB) and American National Standards Institute (ANSI), heard a cry for partnership on the topics of identity management, identity theft measurements, and data breaches. As a result a working group developed

through a collaboration of more than 70 organizations from public and private sectors. This group became the Identity Theft Prevention and Identity Management Standards Panel (IDSP). The IDSP has been responsible for two major reports. The first report considered the entire life cycle of identity management and concluded by providing business and government entities recommendations for areas needing new standards. One significant recommendation was the need to "create uniform guidance for organizations on data breach notification and remediation" (ANSI, 2008).

The second report was released by the IDSP in 2009 and "as part of this effort, a working group was convened to review published research on identity theft and data breach trends, identity theft protection services and information security solutions" (J. McCabe, 2010). This working group was led by Rick Kam, President and Co-Founder of ID Experts, the researcher, and the ID Experts team. The working group catalogued 166 research studies over an eight-week period. The group analyzed methodologies for studying identity theft, and related concepts such as data breach, with the goal of discovering potential disparities in the way key terms are defined in statute versus in practice (IDSP, 2009).

The group observed some contradictory results in research findings attributable to differences in terminology, research methodology, and even potential bias in research sponsorship. "It also noted a number of gaps in existing research such as the effects of identity theft versus identity fraud, breach correlation to identity theft, and the effectiveness of identity theft protection services and information security solutions" (J. McCabe, 2010).

Research trio Alessandro Acquisti, Rahul Telang, and Sasha Romanosky of Carnegie Mellon University, published a working paper on the efficacy of notification laws. The researchers sought to estimate the impact of data breach disclosure laws on identity theft

over a four-year period. Survey results found no "statistically significant effect that the laws reduce identity theft," even after considering income, urbanization, the strictness of law and interstate commerce. Their findings suggest that the probability of becoming a victim of identity theft, conditional on a data breach, is very small (Acquisti, Telang, & Romanosky, 2008).

Generally speaking, consumers support data breach notification laws and, according to an AARP survey, think data breach notification legislation is important. So much so, in fact, they indicated "they would not only support it [legislation] but would be more likely to vote for a candidate that supported such legislation" (Guengerich & Nelson, 2008). However, the survey did not ask consumers about their perceptions of the advice given to them as a result of data breach legislation, or how informative that information may or may not be.

In 2007, Senator Patrick Leahy's (D-VT) office introduced the concept of "over-notification". His office's report to congress claimed, "The question of over-notification has been raised by industry participants. Business groups argue that the California breach notification law has prompted over-notification (companies notifying consumers of data security breaches when there is no risk of economic harm or fraud)" (Stevens, 2007). The phenomenon known as over-notification has taken on a dramatic new meaning as the legislative framework has evolved in the last eight years.

Some policy makers and their constituents argue that consumers are becoming desensitized to data breach notification letters simply due to the volume they receive. This might be an unintended consequence of notification laws designed to alert and inform consumers their information has been compromised. For example, just in 2009, Maryland

residents (whose state Attorney General, Douglas Gansler (D-MD), posts notice letters on his website: http://www.oag.state.md.us/idtheft/breacheNotices.htm) had received well over 150 individual data breach notification letters.

Ann Cavoukian, Ph.D., Information and Privacy Commissioner for Ontario, Canada, agrees that "A tension exists between too little and too much notification, and with it socially optimal levels of security and privacy protections" (Cavoukian, 2009). The researcher also took the opportunity to interview Leahy's office on the current state of the over-notification concerns, and staff agreed that it was "a bigger issue six years ago than it is today. The bigger concern now is a need for national standards and providing consumers information which they can act upon" (L. Grigsby, 2010).

METHODOLOGY REVIEW

This research project has two distinct components. The primary research was conducted by a working group of academics, professionals, and industry thought leaders whose mission was to inventory related research about "measuring identity theft," and to document the findings. The secondary research consists of the researcher's independent examination of data breach responses, and the reactions and perception of the individuals affected by them.

Primary Research – IDSP

In the last few years, identity theft has become one of "the nation's most prominent marketplace issues" and a significant threat to commerce (IDSP, 2008). This concern prompted the BBB and ANSI to create a new market-wide initiative that would help arm businesses and other organizations with the tools necessary to combat identity theft and fraud, thereby protecting consumers, and ultimately themselves from the risks associated with such crimes.

On September 13, 2006, the IDSP was commissioned. This specific workshop was convened because of a "concern that controversies about research methodologies make it difficult to measure how well the marketplace is doing in combating identity crime, posing a challenge to industry, law enforcement and consumers" (ANSI, 2009). The IDSP is comprised of a diverse mix of private and public sector participants. The IDSP charged itself with cataloguing existing standards, guidelines, best practices, and related compliance systems germane to identity theft across all market sectors and industries, and published the findings as a "one-stop resource," a compilation, which did not previously exist (ANSI, 2009).

In 2009, the researcher was invited to join the IDSP working group. The IDSP had come to realize that expertise regarding data breach issues was a necessary component to its overall mission. The working group's mission was to create an inventory of available and related research, position papers, white papers, analysis, and findings existing in the data breach field. The research spanned the most recent five years from February 2004 through May 2009. The final IDSP report was published on October 20, 2009. Because of the researcher's concentration, she continued to compile research through year end, December, 2009.

The group compiled an inventory on four key areas of interest: identity theft, data breach trends, identity theft protection services, and information security solutions. The panel started with the sample list of 15 research studies that were identified and published in an earlier IDSP report (IDSP, 2008). Existing and new members of this group exchanged information about known research work eventually arriving at a total of 166 studies (IDSP, 2009). The group recognized that research is being published on a weekly basis.

The group considered several questions in its analysis of the studies:

- What current research studies exist that measure identity theft? Data breaches? Identity theft protection services? Information security solutions?
- Are there similarities or differences in the conclusions of this research? If so, what can that be attributed to?
- Are the differences causing marketplace confusion?
- Is there a discernable relationship between methodology and outcome?

- Is there a need for additional research on measuring the various facets of identity theft?

The group also considered whether or not there were conflicting findings in the research and whether or not there were any opportunities where additional research would be useful. Finally, the group offered some observations on what makes a research study useful, such as disclosing research methodology, sources of funding and potential limitations of the methodology, and clearly identifying the intended audience and the problem it is addressing. The full report is available at: http://webstore.ansi.org/identitytheft (J. McCabe, personal communication, March 4, 2010).

IDSP Collected Data. The data collected came from 166 studies and the group decided to create a table to sort the research into the four primary categories. The working group used the category labeled "Other" to include opinion papers that did not fall neatly into the primary categories (IDSP 2009). Table 1 illustrates the five C*ategories of Research* that were developed:

Table 1. Categories of Research

Categories of Research	# of Studies
1. ID Theft	72
2. Data Breach	28
3. ID Theft Protection Services	21
4. Information Security Solutions	41
5. Other	4
Total	166

The next step was for the research to be put into an inventory form that was meaningful and consistent. Appendix A contains a list of fields included on the I*nventory Working Sheets*, (See copy of comprehensive list of fields included in the inventory working

sheets at Appendix A) and the common description associated with each one. Once this was completed, the group broke up into subgroups, each to manage one of the four primary categories. The category the researcher co-chaired for further analysis was the data breach research category. Within the primary categories, four subcategories were defined to help further group and compare the various research studies. The subcategories the data breach research group developed were:

1. Consumer impact
2. Business impact
3. Risk
4. Trends and patterns

Table 2, represents the research within the *Data Breach Research* category and use of these subcategories to group related studies:

Table 2. Data Breach Research (sorted by proposed subcategory)

Item #	Researcher	Title of Study	Proposed Subcategory	ID theft defined?
12	PWC	Information security breach survey 2006	Business Impact	Yes
1	Forrester	Calculating the cost of a security breach	Business Impact	Yes
4	Ponemon, PGP, Vontu	2007 Annual study: cost of a data breach	Business Impact	Yes
19	CMU	Is there a cost to privacy breaches? An event study	Business Impact	No
11	Javelin	Consumer survey on data breach notification	Consumer Impact	Yes
18	Gartner	Frequency of data security lapses increased cyber risk attacks damage consumer trust in online commerce	Consumer Impact	Yes
6	AARP	Opinions of AARP members in West VA about breach notification legislation	Consumer Impact	No
15	Ponemon	Consumer response to data breach notification	Consumer Impact	Yes
13	Insight Express	The challenge of data leakage for businesses and employees around the world	Consumer Impact	Yes
5	Ponemon	Results of assessing the business impact of a data breach	Consumer Impact	Yes
2	GAO	Data breaches are frequent, but evidence of resulting theft limited	Risk	Yes
10	British Telecom	ID theft risk: huge amount of sensitive data still on redundant computer disks	Risk	No
16	Cendant Tech	Data hung out to dry: 9,000 USB's left at dry cleaners	Risk	No
17	Gartner	2008 data breaches and financial crimes scare consumers away	Risk	Yes
3	ID Analytics	Data breach harm analysis uncovers new patters of misuse	Trends	Yes
9	CMU	Do data breach laws reduce ID theft	Trends	No
8	Verizon	2008 Data breach investigation report	Trends	Yes
7	AARP	Into the Breach: Security Breaches and ID theft	Trends	Yes
14	Hunton & Williams	Dos and don'ts of data breach and information security policy	Trends	No

The researcher utilized this process and format to continue building the inventory through year end 2009; at which time an additional 16 pieces were added, totaling 182 inventory elements.

The ANSI/IDSP report relevant to the data breach research topic includes an inventory of 28 independent pieces of research. The report finds that of these: (a) 72% of the studies disclosed the methodology; (b) 66% of the studies identified the size of the population in reference; and, (c) 52% of the studies included a definition of identity theft (IDSP, 2009 Part 4.3 section B).

The group examined the research based on the criteria outlined by the working group. It should be noted that the group did not generally observe contradictory results but, it was absolutely determined there were gaps in the existing body of knowledge. Some of these include (IDSP, 2009 Part 4.4 section B): (a) breach correlation to identity theft (e.g., identity crimes, medical employment, other); (b) efficacy of existing laws (e.g., credit freeze laws, breach notification laws); and, (c) whether a comprehensive breach response limits legal liability and cost.

What Makes a Study Useful?

One of the most useful aspects to the working group consensus process was in addressing the question, *What Makes a Study Useful*? This concept provided helpful information for readers of this report who may be developing different methodologies for a new study. This list was not meant to identify specific research studies or call out a specific organization's work. Following is a list of the group consensus (IDSP Part 4.5 2009):

- The methodology is disclosed along with caveats, biases, and limitations.

- The report clearly identifies the intended audience and the problem it is addressing.
- The authors provide actionable suggestions if appropriate.
- The observations illustrate either patterns or trends.
- It is easy to read and understand.
- The report is accessible, whether it is free or fee-based access.
- The organization that performed the research is credible.
- The report contains detailed findings (e.g., on victimization, criminalization patterns, and trends).

IDSP Report Findings

The final report was released on October 20, 2009. The highlights include a: (a) comparison of how key identity theft and fraud terms are defined in statute and in research surveys with a discussion of why they are sometimes different; (b) a catalogue of 166 research studies on identity theft and data breach trends, identity theft protection services and information security solutions, with notes on contradictory research findings, gaps in existing research, and observations on what makes a study useful; and, (c) recommendation that identity crime research that is publicized or intended to shape public policy should include a lexicon of significant terms and a methodology statement, with specific elements of the methodology statement defined (IDSP, 2009).

This report and its findings have been invaluable to the researcher as she undertook further research, and prepared to embark on the secondary research project.

Secondary Research: The Applied Research Project

There were three objectives of the secondary applied-research component. The first objective was to determine how individuals affected by data breaches react to data breach notification letters. The second objective was to understand if individuals changed the way they do business with the notifying organization. Based on information in the notification letter, the final objective was to determine whether affected individuals took independent actions to protect themselves from falling victim to identity thieves.

The researcher explored these objectives by deploying and dispatching a survey. For purposes of this project, *subscribers* will be defined as individuals who for a fee, elect identity theft protection services with ID Experts. The *sample population* will be defined as those subscribers who were selected by the researcher to be given the opportunity to participate in the research project survey. *Survey participants* will be defined as those within the sample population who actually completed the survey. *Qualified participants* and *participants* will be defined as those survey participants who met researcher's criteria as defined in the survey.

The researcher's objectives relate to an important and significant controversy between businesses, legislators, and privacy rights groups over the theory of "over-notification." Privacy rights groups argue that it is important to inform individuals whenever there is a breach of personal information. Businesses and some legislators argue that notification becomes less effective if individuals become overcome with too many of them (Stevens, 2007). This research will seek to prove whether over-notification is an issue for key stakeholders or not.

Finally, the researcher will examine the responses of the survey participants to determine their perception upon receiving a data breach notification letter, and if receipt of the letter caused survey participants to change the way they do business with the organization who experienced the data breach.

The researcher and the organization she represents have a deep obligation and commitment to the protection of personal information. To ensure the quality of input and response, the study was conducted anonymously. No personally identifiable information was sought or included in the study report or provided to the researcher. Survey participants did so voluntarily and did not receive payment or benefit because of their participation. Risks of harm to ID Experts subscribers was no more than commonly experienced in the normal course of business.

With approval from her employer, ID Experts, an identity theft protection service located at 1 Lincoln Center 10300 SW Greenburg Road, Suite 570 Portland, OR 97223, the researcher selected a subset of subscribers in the employer's database. This sample population consisted of 536 subscribers from across the country and from varying demographics. Upon completion of this query, the ID Experts Members Services team communicated with the sample population on behalf of the researcher. The researcher and the research project were introduced to the sample population electronically, but the researcher had no direct contact with the population. Surveys were delivered electronically via SurveyMonkey®.

An email was dispatched to the sample population by ID Experts (See Email to Participants at Appendix B). This email included an informed consent notification to allow the sample population to understand how this information would be used (See copy of

Informed Consent Notification at Appendix C), and the survey questions (See copy of Survey Questions at Appendix D).

Once the results were collected, they were analyzed to determine whether survey participants who had received notification letters were concerned about them, and how receipt of such a letter caused them to react. The researcher analyzed the results to answer the following questions:

- Do notice letters help or hinder the individual's ability to protect themselves from fraud?
- Is there even a correlation between data breaches and identity theft and, if so, how do they correlate?
- Were survey participants experiencing over notification?
- Do the survey participants even recall the name of the entity that sent them the letter?

Did receiving the letter cause the individual to change the way they conduct business with the entity? The research hypothesis has several parts, which will all be examined in more depth. Primarily, the researcher was interested in individual perceptions, deterioration of a company's image, and over-notification. In order for the data to support the hypothesis, there were a few factors that needed to be considered:

- Had the survey participant been the recipient of one or more notification letters? (Participants who had not received at least one notification letter in the twelve months preceding receipt of the survey were excluded from analysis).

- Did survey participants recall the name of the business where their personal information was compromised? (The researcher is keenly interested in learning if data breaches have the potential to damage a company's image. It was critical to analyze how a recipient of a notification letter perceived the letter and whether they even knew who sent it to them).

What kind of response did survey participants have to notification letters? (Studies show that "over-notification" is causing consumers to become desensitized to notification letters simply due the volume they receive.)

Research Hypothesis

Identity theft has been called the fastest growing crime of our decade. Does all the attention placed on data breach notification and the associated regulations many states have adopted have any impact on the consumers they are intended to protect? Despite public outcry for stricter standards in managing personal information, data breaches continue to occur (ITRC, 2010a). Policy makers in at least 45 states have responded by enacting hundreds of laws intended to combat identity theft and in support of data breach notification. Does complying with these laws and providing individuals with notice that their information has been lost give consumers any personal advantage in preventing identity theft (Acquisti, Telang, & Romanosky, 2008)? Does notifying an individual of the loss of their personal information damage a company's image or brand? Are we in fact making things worse by over-notifying consumers (Stevens, 2007)?

Notification Letters. Data breach notification letters may provide benefits to consumers aside from potentially reducing their risk of falling victim to identity thieves. The

purpose of the research is to understand individual's perceptions about this. The researcher anonymously surveyed 536 individuals utilizing an electronic delivery tool called Survey Monkey, and asked each participant a series of up to 16 questions.

These questions were designed to help the researcher evaluate the perceptions of these individuals. The researcher examined common perceptions about data breach notification and compare that to the research results. The researcher sought to determine if there were additional benefits to consumers who receive data breach notification letters, such as heightened personal awareness of identity fraud and common services to protect individuals against identity-related crimes, and increased understanding of risks related to the events that trigger notification letters.

Research Objectives. The main theme of this research consisted of three overall objectives (although one question led to another in the researcher's mind). The first objective was to find a way to measure an individual's response upon receipt of a notification letter, determining how the individual reacted, how they perceived the contents of the letter, and ultimately whether they modified their behavior as a result of reading the letter. The second objective was to better understand the individual's behavior change, if any, and whether the individual changed the way they did business with the entity that lost their personal information. The final objective was to determine whether individuals perceived the letters as helpful in offering protection mechanisms, and to determine if, as a result of receiving these letters, the affected populations took actions to protect themselves against identity theft.

Research Thoughts. The researcher hypothesized that individuals who received notification letters would feel anxious about the organization that sent them. This anxiety contributes to consumers overreacting and in some cases changing the way they do business

with the organization that lost their data. There is a certain element of *hysteria* that can arise in a widely publicized breach particularly if it affects a large population. Furthermore, while "over-notification" is not really a problem, notification letters are confusing, do not offer helpful suggestions to consumers, and do not help recipients to prevent identity theft (Ponemon, 2008). Effectively crafted notification letters however, might help individuals to feel better informed about identity theft, and the threats presented to them when an organization loses their personal information. The effectiveness of these letters was questioned by the researcher, who thinks that credit monitoring has become a de facto service offered to these individuals, and suggestions offered may not fully prevent consumers from falling victim to identity theft as a result of the data breach. Other points explored in the research included:

- There is little support that the phenomenon known as "over-notification" actually exists.
- Clear communication in notification letters helps contribute to positive outcomes for the organization. There may be a direct correlation between data breach response and lost business for the organization responsible.
- The content of notification letters might be lacking, therefore contributing to anxiety and confusion. However, most notification letters are simply to notify the consumer of the incident. A lack of recommendation in the notification letter contributes to anxiety and confusion for the sample population.
- Credit monitoring seems to have become a *de facto* service offered for data breach response.

- Data breaches lead to lost revenues caused by customer turnover, and caused the sample population change the way they do business with an organization after being notified of a breach.
- Data breach notification letters help educate consumers and contribute to a heightened awareness about identity theft, allowing individuals to better protect their personal information from actual theft and misuse.
- Effective notification helps the sample population "take precautions" that contribute to prevention of identity theft victimization.
- Data breaches cause people to become victims of identity theft.

Research Subjects

ID Experts maintains a list of subscribers to its services. These subscribers are U.S. residents; who have either "opted-in" to or "opted-out" of receiving communications from ID Experts when they registered. The researcher made certain to only include subscribers who opted in. The researcher has no known relationship to the subscribers, or the sample population selected and, the survey was performed anonymously. Subscribers who utilize ID Expert's services as a result of a data breach were excluded from the sample population, as were subscribers from groups in which such a request would not be in keeping with that group's privacy policies.

Email Dispatched to Participants. A total of 536 eligible subscribers received the email request to participate in the survey on December 17, 2009. The sample population was chosen at random to enable the researcher to reasonably state the population represents adults age 18 and over, from multiple geographical locations within the U.S., of both genders.

Upon receipt of the email, the sample population was introduced to the researcher and the research project and encouraged to complete the survey which was accessible through an internet hyperlink.

The Survey. Once the survey participant clicked on the hyperlink, they were immediately directed to the secure SurveyMonkey website which hosted the survey, https://www.surveymonkey.com/s/IDExperts. The 16 questions were designed to allow for the collection of information, without attributing specific responses to any particular individual, making it effectively anonymous. The questions are as follows:

Table 3. Survey Questions

Question 1:	Please confirm you understand the survey is voluntary and anonymous.
Question 2:	In the last 12 months, have you been the recipient of a notification letter alerting you to the fact your personal information was lost or stolen? (Due to a data breach incident)
Question 3:	How many letters like this have you received in the last 12 months?
Question 4:	Regarding the most recent letter you received, do you remember the name of the organization that reportedly lost your information?
Question 5:	Were the circumstances that led to the loss of your personal information clearly explained to you in the most recent letter?
Question 6:	What was your level of concern or anxiety upon receiving the most recent letter?
Question 7:	After reading the most recent letter did you feel better or worse?
Question 8:	The most recent letter I received suggested that I: (Check all that apply)
Question 9:	Did the organization responsible for the loss offer you a complimentary service?
Question 10:	Did you take advantage of the complimentary services that were offered?
Question 11:	After receiving the notification, did you change the way you do business with the organization?
Question 12:	Can you describe the change in the way you do business with this organization?
Question 13:	Did you feel better informed about risks of identity theft because of this letter?
Question 14:	Did this letter help you to better recognize, address, or prevent threats of identity theft?
Question 15:	Do you believe your information was misused as a result of the data loss described in this letter?
Question 16:	Who do you know that has been a victim of identity theft?

The survey was concluded December 25, 2009, at which time the analytic tools within the Survey Monkey application were used to tabulate and graph the collected data.

Data Limitations

The limitations of this research include potential for bias and reliability of self-reported data. Because of these limitations, this study may fall short of providing definitive applied research results. It is the goal of the researcher to interpret the survey findings without bias or influence of her employer, position, or expertise. The goal is to find a balanced way to represent the findings, coupled with analysis of existing research, with some expertise applied, but allowing the basis for conclusions drawn to be from the data collected.

Additionally, any time a survey asks respondents to self-report opinions or experiences about certain concepts, despite the researcher's best efforts to provide common definitions to the participants, there is room for reliability of the data to be an issue. Since this is not the sole source of data in this study, the researcher correlated the survey findings with published research in related areas, to support the researcher's hypothesis. The researcher also found that the response rate of *qualified* participants was somewhat limited in volume, probably contributing to limited analysis.

Finally, while individuals should feel comfortable being honest in responding to the survey questions, the responses are likely to be reliant upon the participant's memory of events and letter content. The researcher intended to reduce this problem by asking the opinions only of individuals who have been the recipient of such a letter in the 12 months preceding the survey (December 17, 2008 through December 17, 2009). A qualifying question to this effect was included at the beginning of the survey.

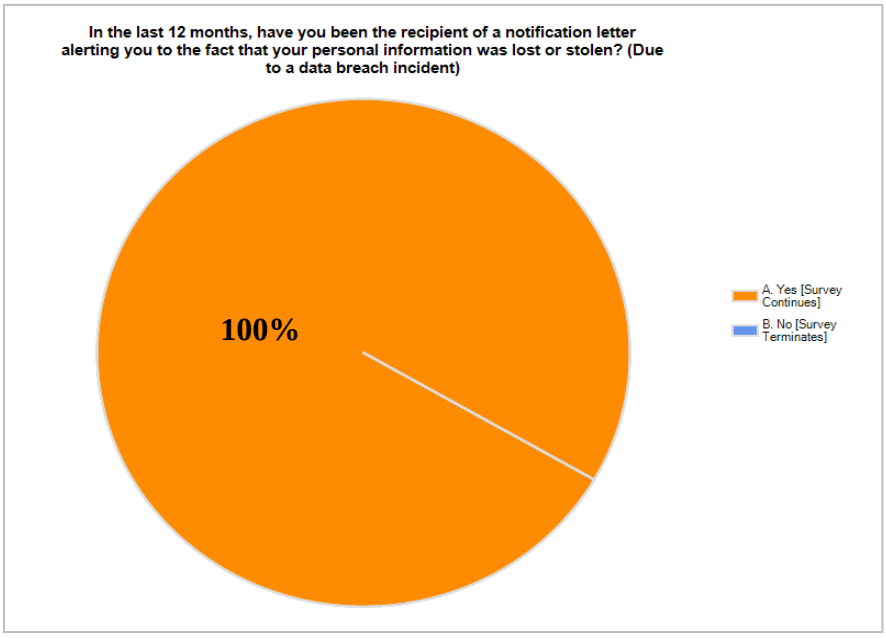
RESEARCH RESULTS

This applied research project has explored the perceptions of survey participants who receive data breach notification letters, by anonymously surveying 536 subscribers and asking them a series of 16 questions. The researcher had a response of slightly less than 10% of the sample population, exactly 50 survey participants in total. Question 1 included the informed consent, in which the survey participants were asked only to proceed if they understood the survey to be completely voluntary and anonymous.

Of the 50 remaining survey participants, two elected not to participate. This left a population size of 48 individuals to proceed to Question 2. Question 2 served as a qualifying question and was presented to participants to ensure that the following two conditions were met:

1. Participant had been the recipient of a data breach notification letter.
2. Participant had received that letter within the 12 months preceding the survey.

Figure 1. Question 2



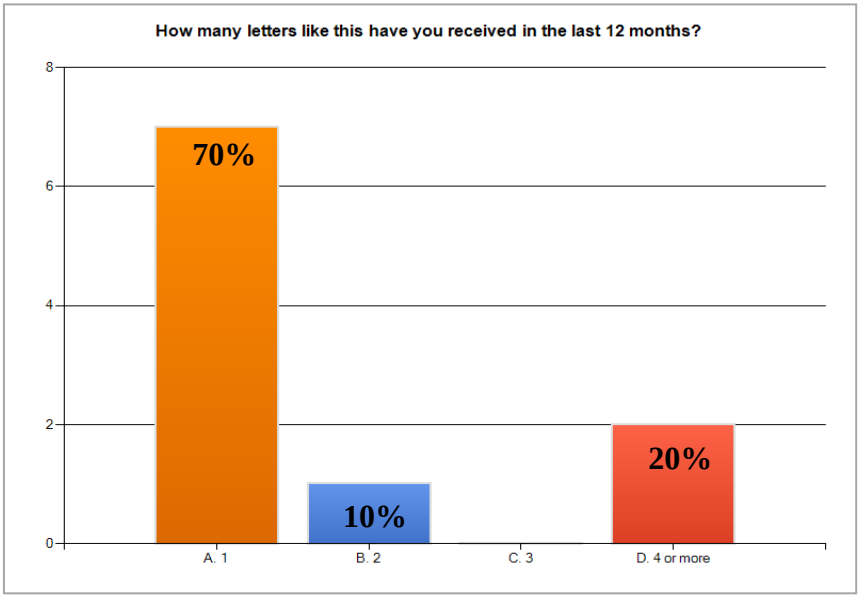
Ten of the 48 survey participants continued the rest of the survey as qualified participants, representing slightly less than 2% of the sample population and approximately 20% of all survey participants.

The researcher discussed the phenomenon of "over-notification" in the literature review portion of this project. The controversy with over-notification is that while lawmakers continue passing notification laws, others feel the notices create apathy amongst the population who receive them, causing individuals to fail to take appropriate precautions to protect themselves from identity theft (Stevens, 2008).

Other experts fear that people may overreact to the notices and take such extreme precautions that their actions will interfere with the timely flow of commerce or affect a business's bottom line. The fact that only10 of the survey participants reported receipt of a notice letter within the past 12 months seems to call into question whether or not this problem even exists.

Further evidence of this was revealed in the survey when qualified participants were asked how many notification letters they had received in the last 12 months. While two participants, representing 20% of the survey participant group, claim to have gotten four or more letters, the vast majority, 70%, had received only one.

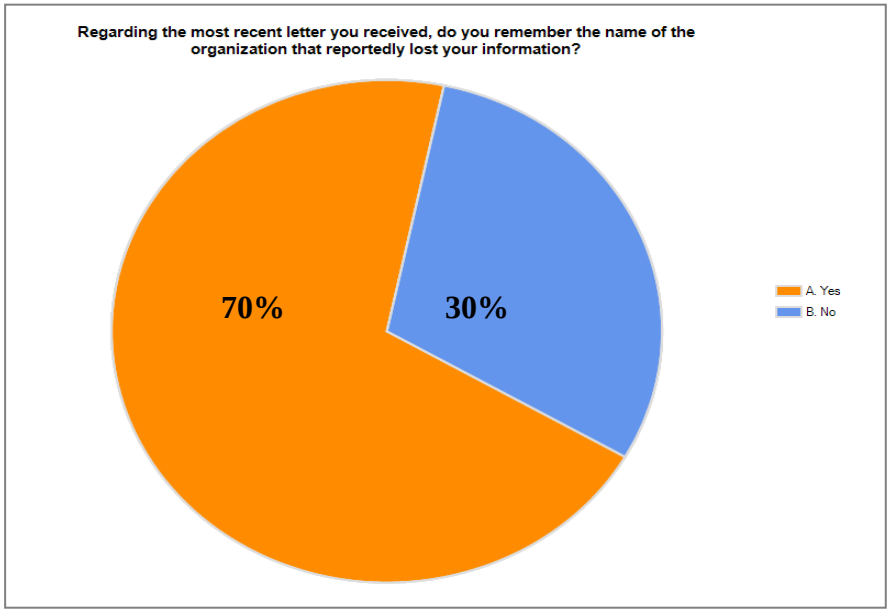
Figure 2. Question 3



Receipt of Recent letters

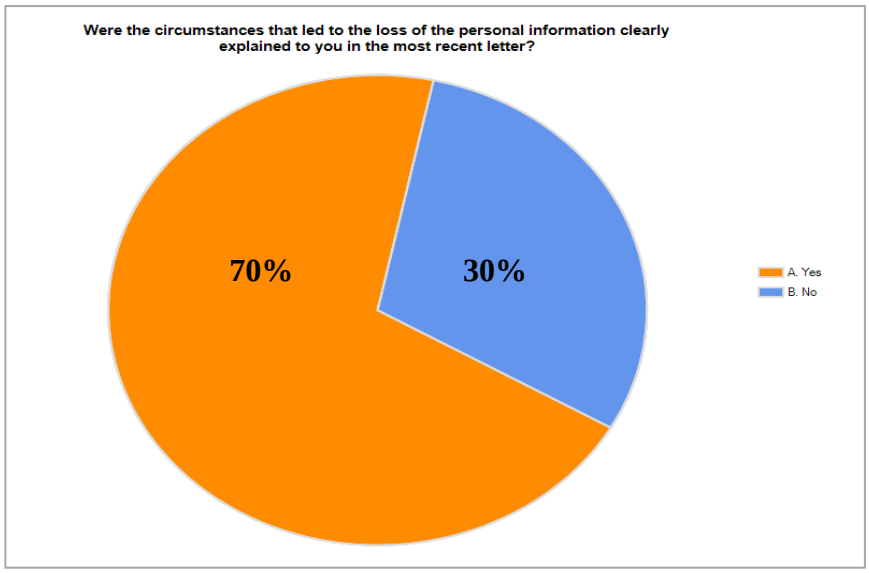
To avoid any confusion, survey participants were asked to recall only the most recent of the letters as they responded to the remainder of the questions. In the most recent letter, a surprising 30% of survey participants could not even recall the name of the organization that sent them the letter. This statistic does not support the researcher's hypothesis that there may be a direct correlation between data breach response and the loss of business for the organization responsible. However, a total of 70% of survey participants did recall the name of the responsible entity.

Figure 3. Question 4



The same percentage of survey participants (70%) shared that the circumstances that led to the loss of their data was clearly explained. This is an interesting result as compared to published research on consumer reactions to data breach notification letters. Other research cites most consumers report finding these letters to be confusing and unhelpful (Ponemon, 2008). The qualifying participant's responses did not support the researcher's hypothesis.

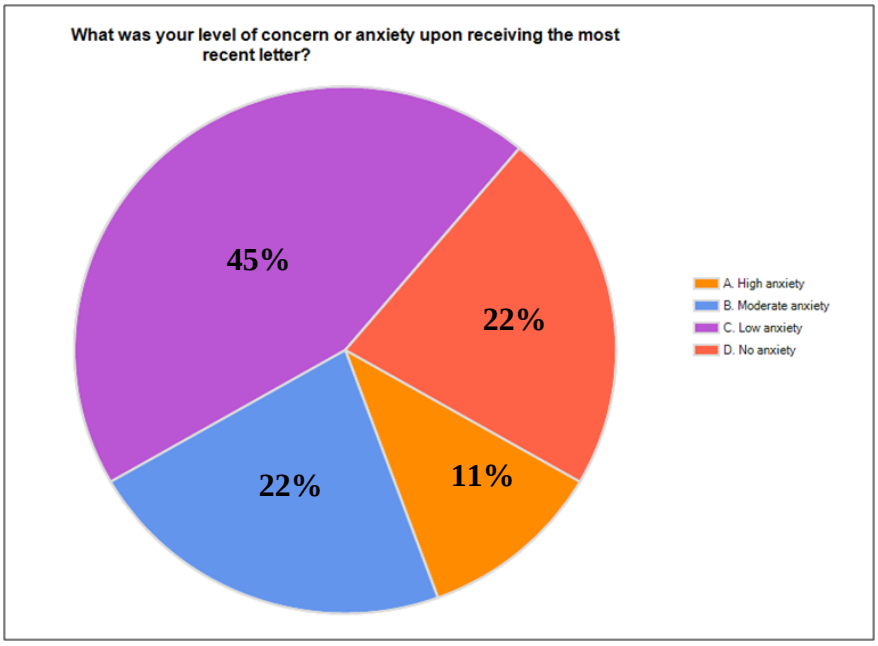
Figure 4. Question 5



Anxiety Response Low

More interesting as it relates to published reports on consumer attitudes and data breaches, was the response to, "What was your level of concern or anxiety upon receiving the most recent letter?" A majority of the qualifying participants, 45% indicated their level of anxiety to be *low*. The fact that almost half of the participants (See figure 5) indicate low anxiety levels upon receiving the notification letter does not support the researcher's hypothesis. In fact, this result indicates notification letters may actually be an effective mechanism for widespread education for individuals affected by a data breach.

Figure 5. Question 6



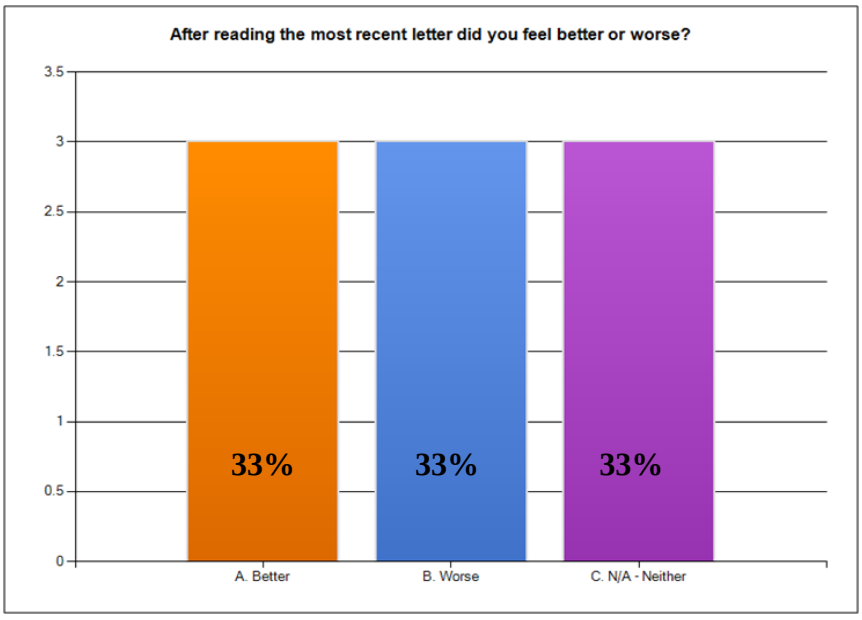
Alternatively, one might conclude that anxiety can be alleviated or avoided through clear and concise information provided in a notification letter that adequately communicates the level of personal risk and provides instruction for protection. The researcher believes that further research specific to this question is necessary. Questioning

the population about their anxiety relative to the letter contents, after better qualifying those letter contents, might help answer this question with more precision.

Participant Feelings

Question 7 asked participants to report how reading the letter(s) made them *feel*. This question was purposely left open so that responses could refer to the organization, or their general state of mind. The researcher was interested in measuring anxiety, and after determining how clearly the letter was written, how this left an individual feeling: better or worse? The results are shown in Figure 6 and speak for themselves, with equal responses across the board. Equal numbers of participants felt better, felt worse, or were indifferent.

Figure 6. Question 7



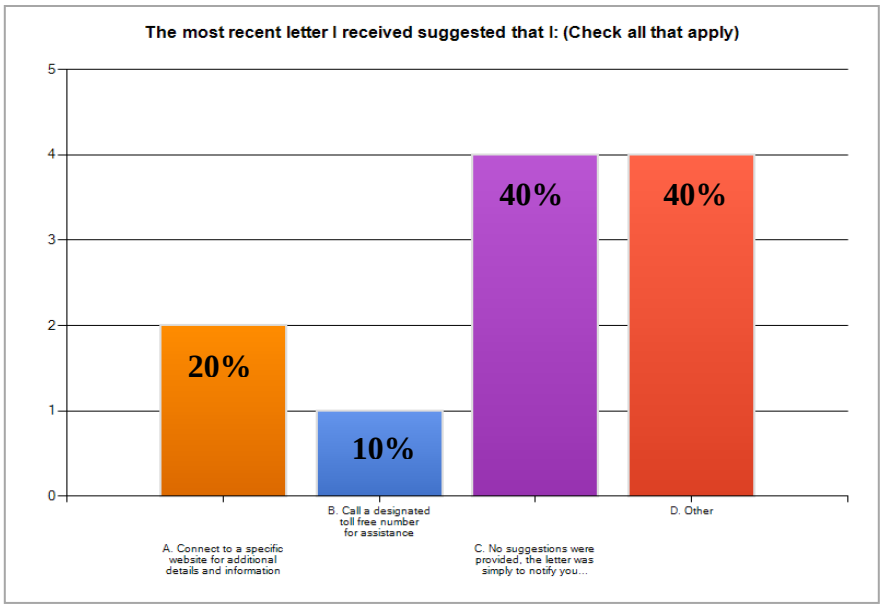
The significance of these findings might again correlate to the quality of the data breach notification letters that survey participants received. Additional research might be warranted about what makes a good notification letter, and better qualification on this detail would be necessary to determine whether or not there is a correlation.

Notification Letter Contents

The next few questions specifically asked about the notification letter contents. Since the responses to these questions rely heavily on the participant's memory, they were asked to reference only to the most recent letter they received. Question 8 asked the participants what suggestions they were given in that letter.

The researcher hypothesized that the content of these letters might be lacking effective substance, therefore contributing to the consumer's anxiety and confusion. A total of 40% of participants shared that they were not provided with any suggestions; the letter was simply to notify them of the data breach and loss of their personal information.

Figure 7. Question 8

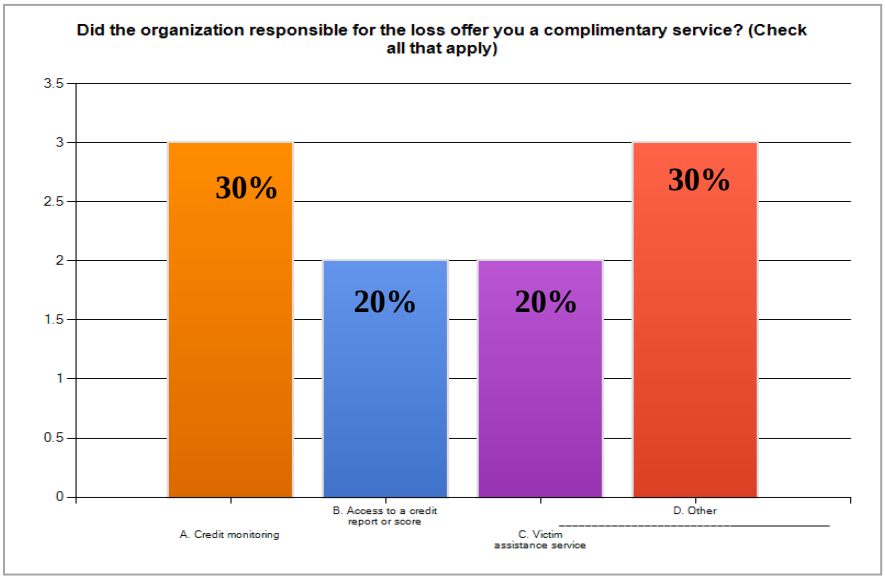


This indirectly supports the researcher's hypothesis, since a lack of recommendations might also contribute to anxiety and confusion. Conversely, a combined 30% indicated they were provided some direction, and were sent to visit an informational website or call a toll-free number for more information. The remaining 40% of participants selected option *other*,

meaning that they received other suggestions. These suggestions varied from placing credit freezes to much more specific "information and instructions needed to protect [oneself]."

Additionally, Question 9 asked the survey participants if they were offered a complimentary service. Figure 8 shows the options and responses, with *other* representing three participants. Two of these them indicated "no services offered" and one participant claimed they were offered "One year of id protection insurance…at no charge." These findings support the researcher's hypothesis that, in fact, credit monitoring seems to have become a *de facto* service offered for data breach response, with the other variations (often provided by the same entities) a close second.

Figure 8. Question 9

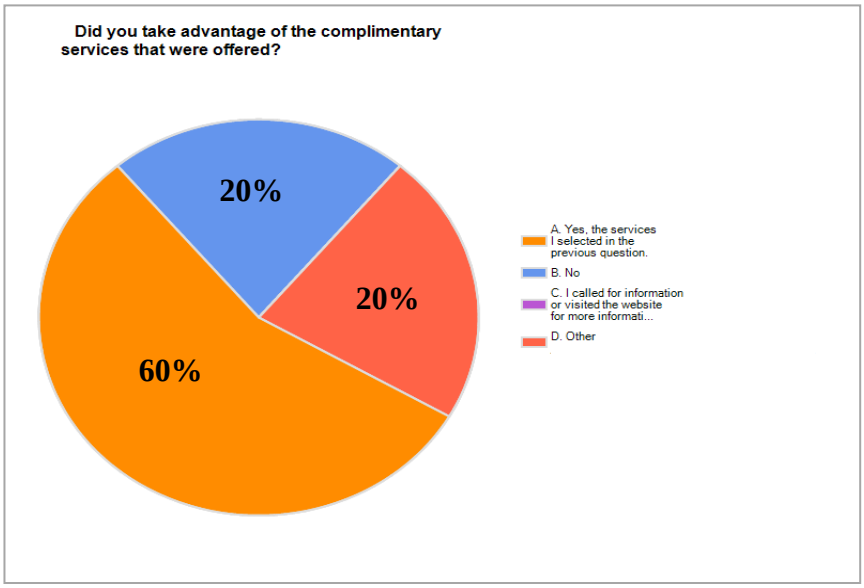


Question 10 asked if they took advantage of the opportunity. Some research suggests that organizations that extend a service offering in their notifications letters fare better with consumers than those who do not (Ponemon, 2008). This same research also suggests that individuals who actually take advantage of service offerings can deliver more positive

outcomes for an organization, compared to impressions from individuals who do not elect to use the service offered.

Figure 9 illustrates the percentage of this population who took advantage of the services offered. More than half (60%) of participants took advantage of the services they were offered. Of the remaining participants, 20% did not utilize services offered, and 20% were not offered any. The fact that a majority of the population were offered services and also took advantage of them might contribute to the reportedly low anxiety level of this group.

Figure 9. Survey Question 10

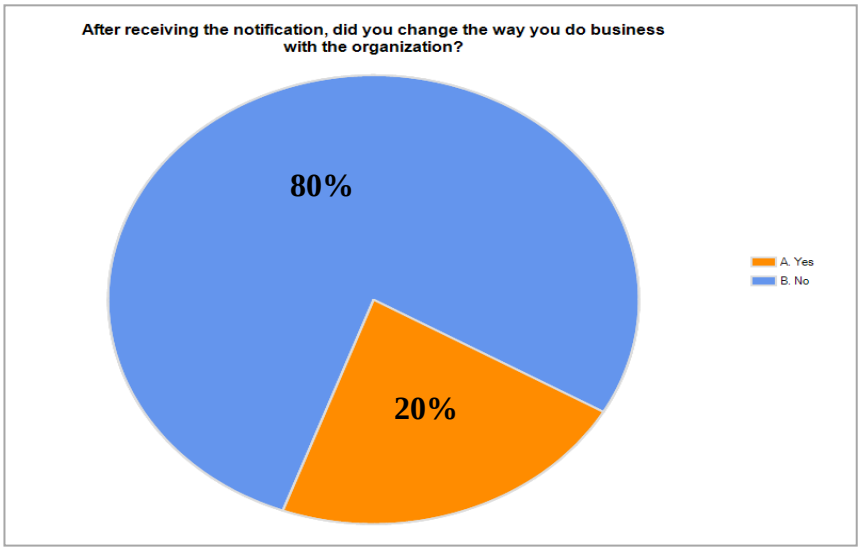


Data Breaches Do Not Cause Consumers to Flee to Other Businesses

The researcher also posed the hypothesis that data breaches led to lost revenues caused by customer turnover and that survey participants changed the way they do business after a company notified them of a data breach. Question 11 asked survey participants if after receipt of the notification letter they changed the way they did business with the organization responsible. The responses to this question were the most surprising of all to the researcher.

A total of 80% of survey participants indicated they did not change the way they did business with the organization responsible for losing their data.

Figure 10. Survey Question 11



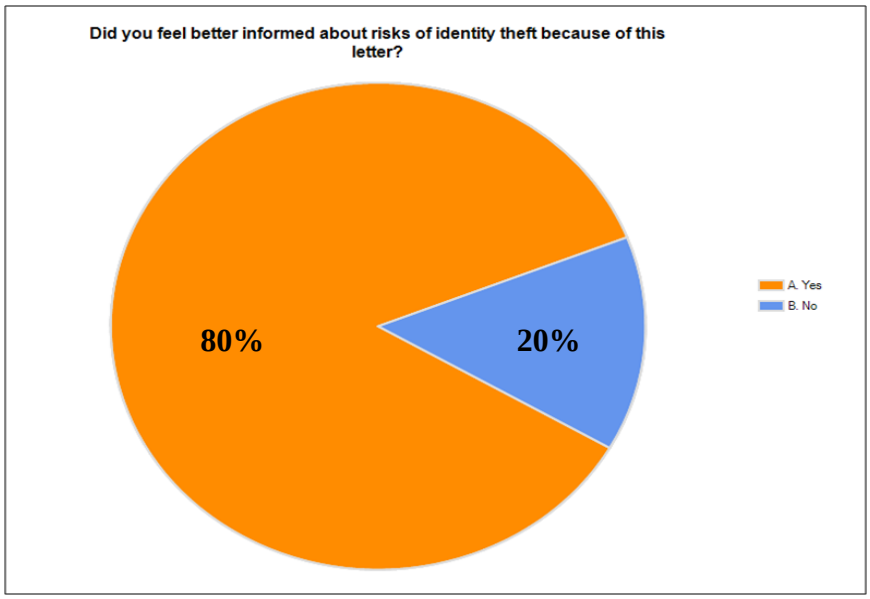
As a follow up, Question 12 asked only the 20% who indicated *yes* in Question 11 to describe *how* they may have changed the way they do business with the organization after receiving notification about a breach. Responses varied, but only one of the participants claimed that change included "…refusal to shop there with a credit card anymore & will only shop there with cash, if at all. I also will not participate in any of their mailings or customer programs."

The researcher suggests that this area of study would benefit from additional research. For example, this researcher did not ask about the *type* of organization responsible for the data breach. In some cases, a consumer may not have a choice about whether to take their business elsewhere (for example, a government agency or long-term loan). Were the researcher to ask individuals to classify the organizations discussed in the survey, there could have been a different outcome.

Notification Letters Provide Victims Good Information

Survey participants were asked general questions regarding identity theft threats in Questions 13 and 14. The responses to these questions would either support or refute the researcher's hypothesis that data breach notification letters help educate consumers and contribute to a heightened awareness about identity theft, allowing survey participants, and individuals in general, to better protect their personal information from actual theft and misuse.

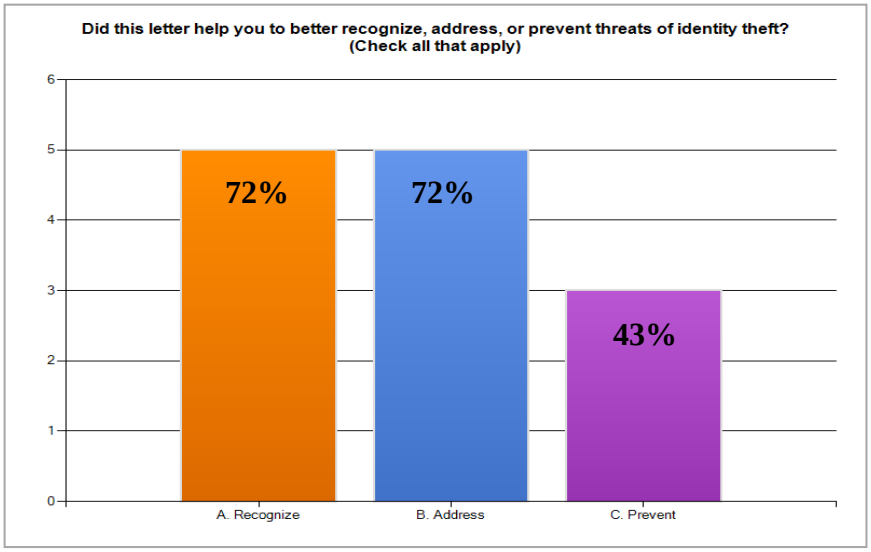
Figure 11. Survey Question 13



As one can see the majority of participants, 80%, indicated they were better informed about the risks of identity theft because of the letter they received. This is important and may be a good candidate for future study, to determine if clear notification helps an organization arrive at this positive outcome. Some research suggests that organizations that extend a service offering in their notification letters fare better with consumers than those that do not (Ponemon, 2008).

To clarify responses to Question 13, Question 14 asked participants about recognizing, addressing, and preventing the threats of identity theft. While survey participants were given the opportunity to select more than one option to this question, more than 70% selected options indicating they were better prepared to "recognize" and "address" identity theft threats. Only three survey participants indicated they were better prepared to "prevent" the threats associated with identity theft.

Figure 12. Survey Question 14



Notification Letters Help Victims Take Precautions

One research hypothesis considered whether notification letters might help survey participants "take precautions" that contribute to prevention of identity theft. However, this researcher's findings do not support that claim. What they might point to, however, is the fact that well-written letters can help to balance these three ways consumers are better educated about identity theft threats. This is significant because it might mean that clear communications in notification letters leads to more positive results. In addition, consumers

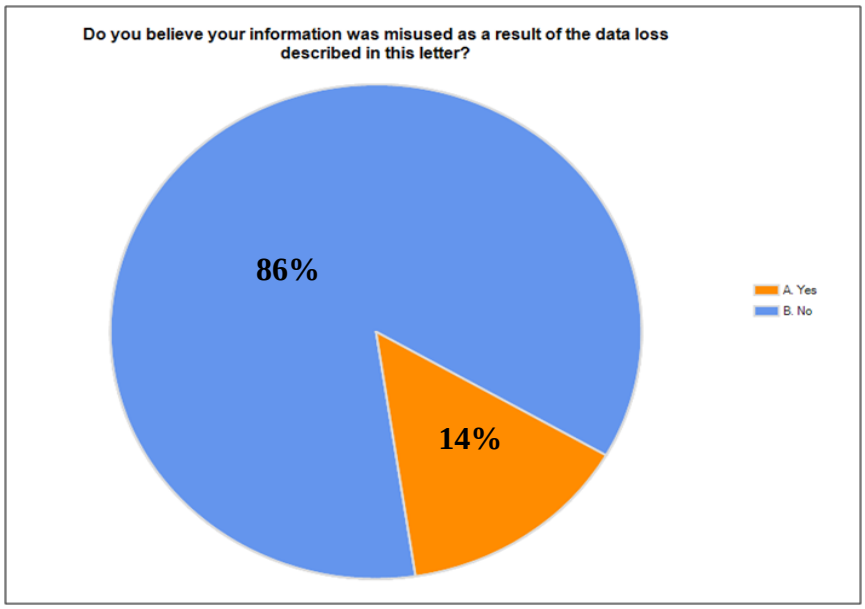
might also realize there is little they can do to actually prevent misuse of their personal information.

Does a Data Breach Correlate to Identity Theft?

Finally, as previously discussed, there is a lot of controversy about data breaches in general and the probable correlation to actual identity theft. According to the Fair and Accurate Credit Transactions act of 2003, Identity Theft means "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR §603.2 To some consumers, the simple receipt of a notification letter causes them to perceive they should be classified as a victim; but, most experts agree that there must be an actual criminal act perpetrated against an individual before they can be considered to be a victim of identity theft.

Question 15 asked participants if they felt their personal information had actually been misused as a result of the data loss described in their letter. A total of 86% reported that to their knowledge their stolen or lost data had not been used in any identity related crimes. The remaining 14% did claim their information had actually been misused as a result of the data breach, a response that tracks well with other published statistics on this topic (Javelin, 2010).

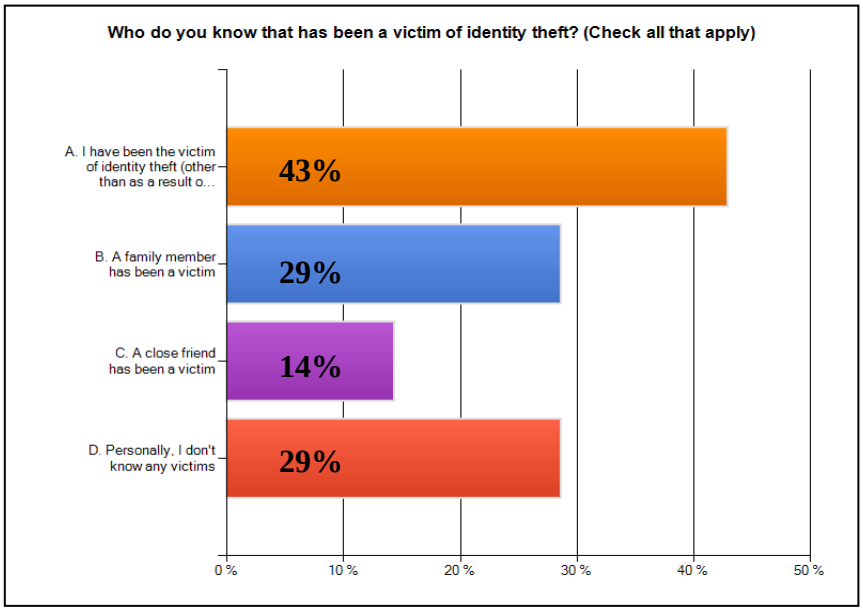
Figure 13. Survey Question 15



Findings in the 2010 Javelin Identity Fraud Survey "reinforce the trend that fraudsters are becoming increasingly savvy with technology and are using personal information stolen in data breaches to open new accounts or to make changes to existing non-card accounts" (Javelin, 2010). This survey also found that victims in the U.S. increased 12% from the previous year to 11.1 million in 2009. With all of the publicized data breaches and the millions of data elements "at large," it would seem logical to correlate data breaches with the rising crime of identity theft.

In Question 16, survey participants were asked about who they might know (including themselves) that was an actual victim of identity theft. Forty-three percent indicated they had been victims due to circumstances *other* than data loss described in the previous question. Once again the researcher qualified the term "victim" to exclude the receipt of a data breach notification letter.

Figure 14. Survey Question 16



Of note as it relates to this finding is the high percentage of individuals who are for one reason or another, victims of identity theft unrelated to data breaches, and unrelated to data breach notification letters. The 2010 statistics indicate that 4.8% of the total U.S. population were victims of identity theft in 2009 (Javelin, 2010). The researcher thought that by properly qualifying the term *victim* and asking survey participants who had received this kind of letter if they had subsequently fallen victim as a result, this theory might be supported. Further research is warranted with better qualified survey questions and populations. It is also important to note that only highly trained professionals can determine with some certainty whether a specific incident relates to a specific crime.

It is becoming best practice to offer victim restoration services to affected populations regardless of whether or not there is a correlation between a victim of a breach incident and actual fraud. Because 43% of the individuals who participated in this survey were identity theft victims, not as a result of the data breach they were notified about, this best practice might be statistically supported.

CONCLUSIONS

There have been many reports, research projects, white papers, and opinion pieces on data breaches. It is an interesting and quickly evolving topic. There are a multitude of laws regulating necessary requirements for organizations who suffer a data breach, and we see best practices constantly emerging in commercial and government sectors.

Lessons learned from examination of existing literature and this researcher's findings are plentiful. Consequences to businesses who report breaches are still costly on many levels, but more research is needed as this concept continues to be measured. Calculating the hard costs associated with responding to a data breach can be mind-boggling, and factoring in the less tangible expenses like organizational reputation might be impossible.

Experts still question any direct correlation between data breaches and identity theft, and many businesses claim that the cost of notifying is excessive. A continued trend intent on preventing identity theft is also apparent. All of these areas are in need of further investigation and research.

Leaders like ANSI may be helpful in creating uniform guidance for organizations and in identifying gaps in existing research; but, there is much more work to be done in determining how consumers perceive data breach events.

This research supports the theory that data breach notification is working to retain customers affected by a breach, revealed that data breach victims are not subject to higher-than-expected incidents of identity related crimes (contingent only upon being affected by a data breach), and have sufficient information to make informed decisions about their next steps when notified that their information has been lost or stolen.

The organizations who implement best practice concepts understand the importance of having a plan of action for a data breach response, and how and when to make effective public notification to customers. Conversely, the lack of planning and a poor data breach response will be costly. Continued research in these areas will be meaningful as we decide how to adapt best practices, guidelines, and formulate policy to further regulate this space.

Appendix A

Comprehensive list of fields included on the inventory working sheets

Comprehensive list of fields included on the inventory working sheets

Field Name	Description
Research Organization	Identifies the organization performing the research
Research Sponsors/partners	Identifies the sponsors and research partners if applicable
Title	Title of the study or report
URL	Web link to access the research
Executive Summary	Executive summary from the report if available
Date Research Published	Date published
Dates of Data Studied	Start and end dates of the research, e.g., 2001 to 2004
Number/Description of Units/Participants Studied	Includes the number of cases in the study, participants, or sources
Quantitative or Qualitative Analysis or Both	Indicates whether the research was quantitative, qualitative, or both
Primary or Secondary Research	Indicates whether the research was primary or secondary
Nationally Representative Sample	Indicates whether the population surveyed was nationally representative
Data Source	Describes data source
Is the Term ID Theft Defined?	Indicates if the term “ID Theft” was defined in the research report
Summary of Caveats/Limitations If Known	Summarizes caveats and limitations or biases of the research
Who was Studied	Indicates who was studied (e.g., consumers, businesses, closed cases, etc.)
Category/Subcategory	Provides categories and subcategories to group and compare similar research studies

Appendix B

Email to Participants

As part of our ongoing efforts to remain the leader in prevention and remediation of identity fraud, ID Experts would like to ask you to participate in a short survey.

Simply click on the link below, and you will be directed to the survey.

ID Experts Data Breach Response Survey

ID Experts is pleased to participate in this applied academic research project. We feel that the more we know the better prepared we are to develop solutions that are meaningful to you – the consumer and a valued ID Experts member.

Your responses and reactions will be collected and analyzed by Christine Arevalo, founding employee and passionate advocate for victims. Your confidentiality and anonymity is assured, and your thoughts sincerely appreciated.

This link will become inactive after one week on December 25, 2009. If you have any questions, please direct them to:

christine.arevalo@idexpertscorp.com

She can provide you with information about the survey, the academic institution which she represents, how the information you share will be used, or a copy of the survey results once they are completed.

christine.arevalo@idexpertscorp.com • ID Experts
1 Lincoln Center 10300 SW Greenburg Road, STE 570
Portland, OR 97223

Appendix C

Informed Consent Notification (Screen shot)

Data Breach Response Survey

Introduction

Thank you for taking the time to participate in the following survey. The survey will take no more than 10 minutes of your time. It will cover 16 multiple choice questions, and be available for the period of one week.

This survey is voluntary and your confidentiality is assured. It is designed to be completely anonymous. If you feel uncomfortable answering a question, you may skip that question. If you feel uncomfortable with the survey you may stop at any time.

*****1. Please confirm you understand the survey is voluntary and anonymous:

Please confirm you understand the survey is voluntary and anonymous: I understand the survey is voluntary and anonymous. [Survey Opens]

I do not understand. [Survey Terminates]

Appendix D

Survey Questions (Screen shot)

Page #2

Survey Qualifier

We are looking for respondents who have been recipients of at least one notification letter within the last 12 months. If you do not meet this criteria you will be directed to the end of the survey.

***2. In the last 12 months, have you been the recipient of a notification letter alerting you to the fact that your personal information was lost or stolen? (Due to a data breach incident)**

- ○ A. Yes [Survey Continues]
- ○ B. No [Survey Terminates]

Page #3

Survey Questions

***3. How many letters like this have you received in the last 12 months?**

- ☐ A. 1
- ☐ B. 2
- ☐ C. 3
- ☐ D. 4 or more

***4. Regarding the most recent letter you received, do you remember the name of the organization that reportedly lost your information?**

- ○ A. Yes
- ○ B. No

***5. Were the circumstances that led to the loss of the personal information clearly explained to you in the most recent letter?**

- ○ A. Yes
- ○ B. No

***6. What was your level of concern or anxiety upon receiving the most recent letter?**

- ○ A. High anxiety
- ○ B. Moderate anxiety
- ○ C. Low anxiety
- ○ D. No anxiety

***7. After reading the most recent letter did you feel better or worse?**

- A. Better
- B. Worse
- C. N/A – Neither

***8. The most recent letter I received suggested that I: (Check all that apply)**

- A. Connect to a specific website for additional details and information
- B. Call a designated toll free number for assistance
- C. No suggestions were provided, the letter was simply to notify you of the personal information loss
- D. Other _____

Other (please specify)

***9. Did the organization responsible for the loss offer you a complimentary service? (Check all that apply)**

- A. Credit monitoring
- B. Access to a credit report or score
- C. Victim assistance service
- D. Other _____

Other (please specify)

***10. Did you take advantage of the complimentary services that were offered?**

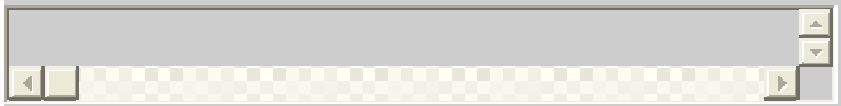
- A. Yes, the services I selected in the previous question.
- B. No
- C. I called for information or visited the website for more information but didn't actually register or sign up for anything.
- D. Other _____

Other (please specify)

***11. After receiving the notification, did you change the way you do business with the organization?**

- A. Yes
- B. No

12. Can you describe the change in the way you do business with this organization?



***13. Did you feel better informed about risks of identity theft because of this letter?**

- A. Yes
- B. No

***14. Did this letter help you to better recognize, address, or prevent threats of identity theft? (Check all that apply)**

- A. Recognize
- B. Address
- C. Prevent

***15. Do you believe your information was misused as a result of the data loss described in this letter?**

- A. Yes
- B. No

***16. Who do you know that has been a victim of identity theft? (Check all that apply)**

- A. I have been the victim of identity theft (other than as a result of the data loss described in the previous question.)
- B. A family member has been a victim
- C. A close friend has been a victim
- D. Personally, I don't know any victims

REFERENCES

Acquisti A., Telang R., & Romanosky S. (2008, September 16). *Do Data Breach Disclosure Laws Reduce Identity Theft?* Retrieved June 14, 2009, from Social Science Research Network Web site: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1268926

American National Standards Institute (ANSI). (2008). *ANSI-BBB IDSP Final Report.* Retrieved January 20, 2010, from http://www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx

CA, Inc. (2008, July 16). *The CA 2008 Security and Privacy Survey*. Retrieved from http://www.ca.com/us/press/release.aspx?cid=180616

Cavoukian, A. (2009, June 24). *A Discussion paper on privacy externalities, security breach notification and the role of independent oversight*. Retrieved November 23, 2009 from http://www.ipc.on.ca/images/Resources/privacy_externalities.pdf

Connecticut Attorney General's Office. (2010, January 20). *Attorney general sues health net for massive security breach involving private medical records and financial information on 446,000 enrollees.* Retrieved January 25, 2010 from http://www.ct.gov/ag/cwp/view.asp?Q=453916&A=3869

Federal Trade Commission (FTC). (2006, January 26). *ChoicePoint Settles Data Security Breach Charges; to Pay $10 Million in Civil Penalties, $5 Million for Consumer Redress* Retrieved July 30, 2009, from Federal Trade Commission Web site: http://www.ftc.gov/opa/2006/01/choicepoint.shtm

Gartner, Inc. (2005, June 23). *Gartner Survey Shows Frequent Data Security Lapses and Increased Cyber Attacks Damage Consumer Trust in Online Commerce.* Retrieved

June 14, 2009, from Gartner Newsroom Web site: http://www.gartner.com/it/page.jsp?id=492157

Guengerich, T., & Nelson, B. (2008, January). *They Want to Know: The Opinions of AARP Members in West Virginia About Data Breach Notification Legislation.* Retrieved June 14, 2009, from AARP Web site: http://www.aarp.org/research/frauds-scams/fraud/wv_data_breach_08.html

Health & Human Services. (2008, July 15). *HHS & Providence resolution agreement*. Retrieved May 3, 2010 from http://www.hhs.gov/ocr/privacy/enforcement/resolution.html

Identity Theft Prevention and Identity Management Standards Panel (IDSP). (2008, January 31). *IDSP Final Report Volume II Standards Inventory.* Retrieved January 31, 2010 from ANSI website: http://publicaa.ansi.org/sites/apdl/ID%20Theft%20Prevention%20and%20ID%20Management%20Standards%20Pa/IDSP%20Report%20Summary.pdf

Identity Theft Prevention and Identity Management Standards Panel (IDSP). (2009, October 20). *IDSP Workshop Report: Measuring Identity Theft*.

Identity Theft Prevention and Identity Management Standards Panel (IDSP): *Report and Webinar*. Retrieved July 9, 2009, from ANSI Web site: http://www.ansi.org/standards_activities/standards_boards_panels/idsp/report_webinar08.aspx?menuid=3

Identity Theft Resource Center (ITRC). (2010a, January). *ITRC Breach Report 2009 Final.* Retrieved January 10, 2010, from Identity Theft Resource Center Web site: http://www.idtheftcenter.org/ITRC%20Breach%20Report%202009.pdf

Identity Theft Resource Center (ITRC). (2010b, January). *ITRC Data Breaches: The Insanity Continues.* Retrieved January 16, 2010, from Identity Theft Resource Center Web site: http://www.idtheftcenter.org/artman2/publish/lib_survey/Breaches_2009.shtml

Kark, K., Stamp, P., Penn, J., & Dill, A. (2007, April 10). *Calculating the Cost of a Security Breach.* Retrieved June 14, 2009, from Forrester Web site: http://www.forrester.com/Research/Document/Excerpt/0,7211,42082,00.html

Javelin Strategy and Research. (2008, June). *Consumer survey on data breach*. Retrieved December 20, 2009 from http://www.debix.com/docs/ Javelin_Research_Consumer_Survey_Data_Breach_Notification_2008.06.pdf

Javelin Strategy and Research. (2009, October). *Data breach notifications: victims face four times higher risk of fraud*. Retrieved from http://www.javelinstrategy.com/ reports/143/221/

Javelin Strategy and Research. (2010, February 10). *2010 Identity Fraud Survey Report.* Retrieved from https://www.javelinstrategy.com/news/831/58/

Ponemon Institute. (2007) *Annual Study: U.S. Cost of a Data Breach - Understanding.* Retrieved Dec 2007, from Vontu Web site: http://www.vontu.com/uploadedfiles/ global/Ponemon-Cost-of-a-Data-Breach-2007.pdf

Ponemon Institute. (2008). *Consumer's Report Card on Data Breach Notification.* Retrieved June 14, 2009, from http://www.idexpertscorp.com/ newsstories/?articleid=169

Ponemon Institute. (2010, January). *2009 Annual Study: Cost of a Data Breach Understanding Financial Impact, Customer Turnover, and Preventive Solutions.*

Stevens, G. (2007, January 25). *CRS report for congress data security: federal legislative approaches*. Retrieved from: https://www.leahy.senate.gov/issues/privacy/data security.pdf

Treanor, J. (2009, July). *HSBC fined £3m for 'careless' handling of customer details.* Retrieved July 20, 2009, from the guardian.co.uk Web site: http://www.guardian.co.uk/business/2009/jul/22/hsbc-lost-data-fsa-fine