

DRAFT
REPORT

Focus Group Report on Consumer
Perspectives on Data Breaches

Prepared for:

Public Interest Advocacy Centre (PIAC)

October 2010

pn 6717



ENVIRONICS
RESEARCH GROUP

33 Bloor St East
Suite 1020
Toronto, ON M4W 3H1

TABLE OF CONTENTS

Introduction	1
Executive Summary	3
Detailed Findings	8

Appendices

- A: Discussion Guide
- B: Recruitment Screener

INTRODUCTION

Background and Research Purpose

The Public Interest Advocacy Centre (PIAC) has undertaken a study of Canadians’ attitudes towards data breaches, and their desired response in terms of notification of the breach, recompense for the breach and likely actions when they are notified of a breach. Currently, the debate on breach notification in Canada lacks consumer perspective. It is expected that this study will result in a recommendation as to the possible scope and content of a breach notification law for Canada which respects as much as possible the desires and concerns of the Canadians whose privacy is breached.

In support of this project, the PIAC engaged Environics Research Group to conduct qualitative research with two target populations, one consisting of Canadians who have experienced a loss or breach of their personal information and been notified of the loss or breach, and one consisting of Canadians who have never suffered such a loss (to their knowledge) and thus never been so notified. This research is designed to explore Canadians’ reactions to a number of key questions and assumptions in the ongoing debate over whether private and public sector actors should notify them if their personal data is lost, stolen or accessed by an unauthorized person, including such key issues as breach notification threshold (e.g., “risk”), timing, manner of notification, to whom notification is made, who should notify and remedies for a breach.

Methodology

A total of four (4) focus group sessions were conducted in Montreal and Calgary, two groups in each city; in each city, one group was conducted with participants drawn from the general public, and one with participants who had personally experienced some form of data breach or ID theft connected to unauthorized access to or use of their personal data.

Location	Date and time	Group composition	Language
Montreal	September 9, 5:30 pm	General public	French
Montreal	September 9, 8:00 pm	Experienced breach/ID theft	French
Calgary	September 15, 5:30 pm	General public	English
Calgary	September 15, 8:00 pm	Experienced breach/ID theft	English

For each session, eight people were recruited with the expectation that six to eight would participate. Each focus group session was approximately two hours in length and was conducted according to a discussion guide developed in consultation with the client team. A \$75 cash incentive was given to each participant in appreciation. (See Appendices for Discussion Guide and Recruitment Screener.)

Derek Leebosh, Vice President, Environics Research Group, acted as Project Director and moderated all focus groups.

All qualitative research work was conducted in accordance with the professional standards established by the Marketing Research and Intelligence Association (MRIA – previously the Professional Market Research Society and the Canadian Association of Market Research Organizations).

Statement of Limitations

The objectives of this research initiative are exploratory and therefore best addressed qualitatively. Such research provides insight into the range of opinions held within a population, rather than the weights of the opinions held, as would be measured in a quantitative study. The results of this type of research should be viewed as indicative rather than projective.

EXECUTIVE SUMMARY

This executive summary presents the key findings of qualitative research conducted by Environics Research group on behalf of the Public Interest Advocacy Centre on the topic of Canadian consumer perspectives on data breaches and notification of the public when such breaches occur. This qualitative research comprised four focus groups (two in Montreal and two in Calgary) conducted on September 9 and 15, 2010, with two target groups: Canadians who have and who have not experienced a data breach, or loss or theft of their personal information.

Awareness, Knowledge and Experiences of Data Breaches

- The predominant image of a data breach involves the intentional “hacking” of computer systems and accessing data, particularly private information, without authorization.
- Most were aware of various publicly reported data breaches that had occurred either locally or on a national level.
- Participants did not distinguish between data breaches happening in an institutional setting where a large number of data records are compromised, and attempts by individuals to fraudulently directly obtain personal information.
- Some fear that the growing tendency toward “over-collection” of data, the sharing of mailing lists, and the low levels of security on many Internet social networking sites are facilitating the incidence of data breaches.
- Many find themselves unaware of how to protect themselves from the consequences of a data breach, and are curious about how such breaches occur and what is done in general to deal with them.
- Participants tended to feel that any organization, from financial institutions to governments to retailers, service providers and employers, that holds personal data on them could be vulnerable to a data breach that would compromise that information.

- Participants identified various consequences that might be faced by individuals affected by a data breach, most notably the potential of financial or other material loss, but also including identity theft that could attach debt, inaccurate health information or even a criminal record to one's name and identity; inconvenience; embarrassment at having personal information made public; possible impacts on personal relationships and employment opportunities; and ongoing uncertainty about what could happen in the future.

Reporting Data Breaches

- Most participants initially assumed that if a company or other organization experienced a data breach that might affect them, they would be informed about it; they felt that if notification was not already a legal requirement, then it should be.
- Participants were divided on whether companies should be required to report all data breaches, regardless of their scope or seriousness. There was general agreement that data breaches involving personal financial data or information that could easily be used to commit identity theft and/or fraud should trigger notification of individuals.
- There was also an acknowledgement that over-reporting of all data breaches regardless of seriousness could have negative unintended consequences such as paranoia and desensitizing people to the risks of serious data breaches.
- Most participants agreed that data breaches involving little chance that the data was actually compromised or involving data that was not likely to pose financial risk should not require notification of individuals. There was, however, a strong preference for some form of central body to which all breaches would be reported in order to keep a public record and to make a determination as to whether the breach warranted broader notification.
- Participants identified a wide range of information involving identity (i.e., SIN), personal finances, lifestyle and personal interests, and Internet activities that they considered sensitive information, but generally considered only personal identity information and financial information, as well as confidential health information, as being sufficiently sensitive to warrant automatic notification.

- Shopping habits and other consumer information were considered personal and possibly sensitive, but only as meriting notification if minors were involved.
- Most participants did not feel that companies and other organizations were capable of making a disinterested decision on whether a breach was serious enough to warrant notification of the individuals affected. Rather, most agreed that decisions concerning notification were best made by a neutral “objective third party” that would not be influenced by concerns about customer perceptions, public image or legal ramifications.
- Most agreed that the Office of the Privacy Commissioner (OPC) – or for some, provincial privacy commissioners working in close concert with the federal body and each other – would be an appropriate choice for a neutral body make decisions on whether a data breach requires notification or other action.
- There was general support for the idea that all breaches should be reported to the OPC, and that a database of such incidents be maintained “for statistical analysis” and made accessible to the public.
- Notification by letter was preferred. Most felt that specific issues should be addressed in such notifications, including: what information was breached; how the breach happened; when the breach occurred; how the breached information could be used; what the organization is doing or plans to do to minimize the risk to those whose information has been compromised; how the breach could affect the individual; what action the individual should take to protect themselves from any consequences; and the name and contact information for a company representative. Some also wanted to be informed of the size and scope of the breach.
- Most participants agreed that if the breach took place when the data was in the possession of a third party acting on behalf of the organization that the individual gave their information to – retailer, employer, bank or financial institution – then notification should come from the organization that the data was initially given to, rather than a subcontracted organization such as a data processor or payroll service.
- Participants generally agreed that, if notification of a data breach were required by law, organizations should face significant fines for non-compliance; some also suggested fines or jail

terms for owners, officers or members of the Board of Directors. Regular oversight to check for further unreported breaches and security audits were also considered appropriate actions.

- Most participants felt that being informed of a data breach would not necessarily mean that they would lose trust or confidence. In fact, some said they would be more likely to sever their relationship with an organization that had experienced a data breach and failed to inform the people affected by it. Full and forthright disclosure accompanied by an indication of steps being taken to minimize the risk of further breaches might even result in some participants having a more positive view of the organization in question.
- Most agreed that the company or organization had a responsibility to take all necessary precautions to ensure that another data breach did not occur, including necessary security updates and changes to procedures.
- Most participants felt that notification of a data breach did not absolve an organization of liability, but at the same time agreed that individuals had a responsibility to take whatever steps were available to them to minimize the effects of the breach.

Alberta Privacy Legislation

- Most participants in Calgary were completely unaware of the existence of any legislation in their province dealing with data breaches.
- After being briefed about the legislation, the consensus was that the Alberta legislation was too weak. Concerns were expressed that self-policing by industry would lead to companies' under-reporting due to conflict of interest.
- Further, participants felt that the standard by which a company was to determine whether it was required to report a specific breach was too vague and open to interpretation; the phrases "reasonable person," "real risk," "significant harm" and "unreasonable delay" were seen as being not clearly defined.

- Participants instead expressed a clear preference for having all breaches reported to the Alberta Information and Privacy Commissioner (AIPC), who would then decide if notification of individuals was necessary.
- Participants tended to think that the goal of the law was primarily “window dressing” in that the government of Alberta was trying to make it appear that they were doing something about the problem of data breaches and how companies deal with them, but that in fact the law was relatively toothless and provided false confidence.
- With respect to the content of notifications, most felt that in addition to the items legally required in the current legislation, it was important for the company making the notification to provide the individual with advice on what steps they can take to reduce any chance of harm.

DETAILED FINDINGS

This report presents the findings of qualitative research conducted by Environics Research group on behalf of the Public Interest Advocacy Centre on the topic of Canadian consumer perspectives on data breaches and notification of the public when such breaches occur. This qualitative research comprised four focus groups (two in Montreal and two in Calgary) conducted on September 9 and 15, 2010, with two target groups: Canadians who have and who have not experienced a data breach, or loss or theft of their personal information.

Topics discussed included: participants' understanding of what a data breach is; general awareness and personal experience of data breaches; participants' knowledge concerning data breaches; the consequences of data breaches for individuals; the obligation of an organization to report data breaches to individuals; opinions of what constitutes "sensitive personal information;" the circumstances under which individuals should be notified of a data breach affecting them; issues surrounding the establishment of an independent body that is notified when breaches occur, and has a mandate to make decisions about notification and to maintain records of all data breaches; the potential role of the Office of the Privacy Commissioner (OPC) in collecting data on data breaches and making decisions about notification; penalties for failure to notify individuals if legally obligated to do so; the effect of notification on customer loyalty; and issues of corporate and personal responsibility with respect to data breaches. Participants in Calgary were also asked to discuss issues surrounding data breaches and notification under the new Alberta legislation.

Awareness, Knowledge and Experiences of Data Breaches

UNDERSTANDING OF THE TERM "DATA BREACH"

Most participants have at least some idea of what a data breach is (generally defined as the loss of or unauthorized access to, or unauthorized disclosure of personal information resulting from a breach of an organization's security safeguards), although most tend to think in terms of "hacking into" computer systems and only later, if at all, consider other kinds of possible data breaches that might involve physical access to hard drives or paper records. The general concept of a data breach tends to be limited to intentional and malicious breaches; accidental or inadvertent breaches are not initially seen as being in the same category.

Some of the ways participants described their understanding of data breaches, top-of-mind, include:

- Somebody's gotten into a piece of data that should be secured, but it's not.
- Anybody getting their hands on your personal information.
- Basically, somebody has accessed your database – whether it's private for yourself individually, or a company, somebody's gotten into it.
- Stolen identity, a type of identity theft.
- Somebody has accessed data that they really shouldn't have accessed, whether or not they forced their way in or not.

AWARENESS OF DATA BREACHES

Personal experiences of data breaches

Almost all of the participants who reported a personal experience with a data breach had experienced credit card or debit card fraud of some kind in which unauthorized charges were made to their card or account. Many had no idea of how their data had been obtained; of those who did, most suspected that their data had been captured at a retail store, but a few mentioned losing their wallet and ID. Several participants mentioned that their cards had been physically cloned, with others; the stolen information was used to transfer funds or make purchases electronically.

Most found out about the incident through their bank or credit card company; a few had cards unexpectedly declined. No one mentioned being informed by a company or organization they were in contact with about a data breach that might affect them.

“It's relatively innocuous, but we got a call from our credit card supplier, our bank, saying, by the way, did you make a \$3,000 or \$4,000 donation to this bank in Nigeria? It seems a little atypical of your behaviour. We were like, no I didn't, actually. They were like, yeah, we didn't think so. It was in that transitional period where the money went in but it didn't clear, so they stopped it immediately. We didn't find out how it happened. They immediately stopped it and everything was fine. But someone obviously had enough access to make the transaction, yeah.”

“We used our card at the plumbing store and we got a phone call from our bank that \$500.00 was taken out from our account. It took us actually a little bit, I can’t remember how long, but some time to get the money back. We didn’t get it right away. They had some cameras in the store, some employees. I don’t know how it was done but it was a PIN. They got the PIN, they got the card. My husband said, you probably scanned it twice or something, do you remember? I don’t remember doing it, but they must have done something.”

One participant, a teacher, mentioned ongoing incidents in which some students have made attempts to hack into the school database in order to change their grades. This participant characterized these incidents as data breaches because “once they get in there, they can access anybody’s file and they can access anybody’s marks.”

General knowledge and awareness

Participants showed a fairly high level of awareness of public reports and media stories about data breaches – most participants were aware of various publicly reported data breaches that had occurred either locally or on a national level, while others mentioned types of data breaches they had heard of without mentioning specific cases.

Some specific incidents mentioned by participants included:

- Medical records from a hospital that should have been shredded being found in a dumpster. (Calgary)
- A laptop left on a park bench by a government employee. (Calgary)
- An abandoned hospital being “imploded” and documents from the mental health unit “flying everywhere.” (Calgary)
- Health cards being stolen or cloned so that people could have surgery. (Calgary)
- Thefts of computers from restaurants to obtain point-of-sale information. (Calgary)
- Financial records left in boxes on the street at branches of the Banque de Montreal and the Banque Nationale. (Montreal)
- Credit card information being hacked from Winners. (Calgary, Montreal)

Participants also mentioned various examples of data breaches and criminal activities that they associate with the idea of fraudulently obtained personal information (whether it is actually obtained through a data breach or through other means):

- Used computers being sold or recycled without having the data on them wiped first. (Montreal, Calgary)
- Collecting CPP by using the identities of people who are deceased. (Calgary)
- Immigrants entering Canada using stolen passport information. (Calgary)
- “Phishing” and other Internet-based scams. (Montreal)
- Fraudulent telemarketing calls that ask for personal information. (Montreal)
- PIN and account numbers being obtained at ATMs. (Calgary)
- Mortgage fraud using stolen identities. (Calgary, Montreal)

In discussing what they know about this topic, most participants tended to focus on the consequences of data breaches and the ways in which breached information could be used. They did not always distinguish between data breaches, where personal data of third parties is compromised, and attempts to fraudulently obtain personal information directly from an individual, such as phishing and schemes in which the perpetrators pretend to be legitimate telephone or door-to-door marketers.

Most participants focused on deliberate attempts to obtain personal information, such as key information for identification purposes (SIN, birth certificate, driver’s licence number, passport number), financial records and health records. They tended to assume that the purpose of the data breach was to obtain information that could be used for financial or other material gain, through the use of this information in ways that ranged from simply using a credit card and PIN number to elaborate instances of complete identity theft.

A few suggested other motivations for breaching data, such as sabotage by disgruntled or former employees, and the “challenge” such activities pose to certain hackers. A few also noted that breaches may not be the result of deliberate attacks on security, but rather may happen through negligence or human error.

Some participants mentioned the growing tendency toward “over-collection” of data, where one is asked to give out personal information in many instances where it is not necessary, thus increasing the likelihood that one’s personal information will be compromised, and making people more likely

to give out personal data through force of habit. Concern was also expressed over the growing tendency by companies to create and sell mailing lists and marketing information.

“You’re seeing a lot more organizations taking that data and making it easy on you. When you go skiing or something, you could have a pass that you can just scan and it automatically debits your credit card when you get on the lift because all that information is stored in their system.”

There was also some discussion about the increasing use by companies – particularly those operating on the Internet – of the “negative option” when adding new features and services, some of which may add significantly to the vulnerability of personal data being exposed, whether to the general public, to potential criminal use, or to marketers. In particular, Facebook was mentioned by a number of participants as an example of social networking sites that are increasingly making it easier for people who are not “friends” or contacts to access private information from the profiles of strangers.

Most participants felt that they did not really know a lot about data breaches, and posed a number of questions:

- What do they want to know – what kind of information is targeted?
- How do they get into the systems – what are the different ways that the data is stolen?
- How do companies constantly protect themselves so they’re not being breached?
- What happens to personal information that is stolen – what is it used for?
- Does the government have a role in helping people prevent that kind of personal breach?
- When are individuals most vulnerable, and what is the public’s role in protecting themselves?
- What are some steps individuals can take to protect themselves?
- What are the trends or security technology features that prevent data breaches?
- Are companies actually getting better at stopping it or are they getting worse?
- How much and how often does it actually happen to a typical consumer in their lifetime?
- If it continually gets worse, are the banks just going to say, enough is enough, we’re not going to give you your money back?
- If there is a data breach, how public is it?
- Does the individual even know when it occurs and how often does it occur?
- When companies keep these records how long do they keep them for?

Participants identified a number of types of organizations that they felt might be vulnerable to a data breach that could affect them, including:

- Banks and insurance companies
- Government agencies
- Revenue Canada
- Credit card companies
- Phone companies or cable companies
- Retail businesses that have large customer databases and loyalty programs
- Airlines
- Employers
- Health providers and hospitals
- Telemarketers

CONSEQUENCES OF DATA BREACHES FOR INDIVIDUALS

Participants identified various consequences that might be faced by individuals affected by a data breach, but for most, the first consequence that comes to mind is the potential for financial or other material loss, from unauthorized charges on a debit or credit card to mortgage fraud in which they might lose their homes. This was true both of those who had been affected by a data breach and those who had not, even though most of those who had been affected had not, in the long run, lost financially, as their banks or credit card companies had either intercepted the unauthorized charges or had been compensated for their losses. There was also a related concern that a data breach could result in someone else running up debt under their name and SIN, resulting in negative consequences to their credit rating and affecting them at some unexpected point in the future.

“I think the biggest concern is financial. Everyone is worried – how does that impact me and what they could steal from you?”

“Impair your ability to get other financial things down the road potentially.”

Participants also mentioned the inconvenience of having to check with one’s financial institutions and credit bureaus, and change personal information from credit card numbers and bank accounts to passports.

Also of concern were various non-financial issues that could arise from identity theft, including having incorrect health records created due to someone else's use of one's health card and the possibility of being faced with a criminal record due to someone else's actions. Other consequences mentioned included the loss of privacy and the potential consequences of having various other kinds of personal information – anything from magazine subscriptions to sexual orientation – made public, ranging from embarrassment to possible consequences on personal relations and employment opportunities.

“I wrote it down as private life versus work life. You're talking about a magazine or toupee or whatever, that's something private that I don't want people to know. I certainly wouldn't want to go to a school and have people know about that. It would be a big taboo, obviously, for me.”

“And then the one other aspect is why people want their health records to remain secure, and that would be if they had a terminal illness that they didn't want anybody to know was happening. Or that they had a mental illness, that they were concerned they wouldn't be able to get a job or that kind of thing.”

“It becomes that kind of a thing and suddenly you don't have a relationship with that person anymore and you're kind of going ‘What the hell happened?’”

A few mentioned ongoing uncertainty about the use of one's personal information as a consequence – knowing that the data is potentially available to others, but not knowing if – or when – it will be used.

“So, for a passport, I'd be concerned for the first five years or however long until the expiry date. My birth certificate and SIN number, those two pieces of information are, I think, the most important pieces of information I have. I'd be concerned for a long, long time because somebody could hold onto that information for a long time before they even wanted to use it because it doesn't change.”

Reporting Data Breaches

OBLIGATIONS OF COMPANY OR INSTITUTION

Most participants initially assumed that if a company or other organization experienced a data breach that might affect them, they would be informed about it. Some thought that this was a legal requirement, particularly for a bank or other financial institution; others were unsure but believed that it was something the organization was morally obligated to do, and would likely do in the interests of good customer relations. Some felt that if notification was not already a legal requirement, then it should be.

Others, however, believed that there was no obligation to report data breaches. A few noted that no organization they had some form of relationship with had ever notified them, or given any indication that they would if such a breach occurred.

Participants were then informed that most provinces – with the exception of Alberta, which recently passed legislation on notification of data breaches, and Ontario, which has a law dealing with breaches of data on health information – have no mandatory laws about notifying anyone that data breaches have occurred, only voluntary codes of conduct. They were also told that data breaches of some sort happen quite frequently and in some cases may be very minor but in others could be much more serious.

Participants were divided on whether companies should be required to report all data breaches, regardless of their scope or seriousness. Some want to be notified, or at least have someone notified, for all breaches involving their personal information; others see different levels of sensitivity of the information in question, or the degree to which something can be done to reduce the consequences, as determinants of whether notification is necessary. Data breaches involving personal financial data or information that could easily be used to commit identity theft were seen as the most serious kinds of breaches, and there was general agreement that notification of individuals should be required for these kinds of breaches.

Many participants, however, did not think that breaches involving little chance that the data was actually compromised (such as a laptop being misplaced for a short period of time) or involving data that was not likely to pose financial risk (such as postal codes) required notification. For some, the

issue was one of inconvenience – they did not want to have to take precautions for minor accidents or breaches which carried very little risk. Others did not want to know about – and worry about – something that was relatively low-risk. These participants talked about “fear-mongering” versus the need to take appropriate steps to minimize risk; they do not want to live in fear of being defrauded or having their identity stolen, but they do need to know when that is a real possibility. Some voiced concerns about the effect on public trust in companies, governments and institutions if all breaches, even minor and non-sensitive ones, are reported to the public.

The point was made that the threshold at which notification should be required varies among individuals: “It’s very subjective – different people consider different things as sensitive enough to be reported.”

SENSITIVE PERSONAL INFORMATION

When asked to list what kinds of personal information might be seen as sensitive, participants mentioned a broad range of things, from standard financial and personal identification data to matters they considered to be parts of their private life that they would not want to be made widely known. These included:

- Social insurance number
- Date of birth
- Driver’s licence number
- Passport number
- Mother’s maiden name
- Fingerprints
- PIN numbers or personal access codes.
- Credit card number or account numbers and information.
- Insurance information
- Real estate or financial assets – RRSPs, stocks, etc.
- Income
- Address
- Telephone number
- Workplace/employer
- Health information, prescription records, health card numbers

- Sexual orientation
- Living arrangements – who you live with
- Criminal records
- Whether one has been a victim of a sexual crime or domestic violence, family and children’s court issues including custody and other similar issues
- Passwords – e-mail, anything used on the net
- Internet service provider and browsing history
- Internet anonymity – avatars, pseudonyms, personas.

There was some ambivalence about breaches involving consumer patterns – some participants said that since it is all being collected anyway and shared with other mailing lists, a breach of this information would be irrelevant, and others simply did not see their shopping habits as being something they need to keep private: “Where I buy my groceries isn’t that big a deal, really.” Others considered this to be, if not necessarily sensitive information, still something that they do not want shared without their knowledge.

“It’s great for the marketing types because they know exactly how to target you and what kind of consumer you are and all that kind of stuff, which is great for them – but I don’t think it’s really any of their business.”

There was much more agreement on breaches involving the shopping patterns of minors. Not only was there concern that this information could be used to target minors in the future when they are “older and making more money and in a better situation for them to take from,” but some worried that knowledge of minors’ shopping habits could be used by pedophiles to stalk and approach them.

CONDITIONS OF NOTIFICATION

There was general agreement that, regardless of what the specific trigger point might be for different people in different situations, there were certain types of data breaches, involving certain types of information that should automatically trigger notification of a breach to the individuals concerned. Most participants agreed that they would want to be notified about a data breach involving important government documents or forms of ID, or a high potential of financial loss. Specific information that all agreed was sensitive enough to warrant notification included:

- Credit card and bank account numbers
- Health records
- SIN
- Birth certificate
- Drivers licence
- Passport number

There was some difference of opinion on what should be done if the data breached is de-identified or encrypted. Most participants in Calgary felt that if the data is sensitive, then notification should be made. These participants tended to feel that “Something that someone can encrypt, someone can unencrypt.” However, a number of participants in Montreal felt that encryption would likely provide sufficient protection that they would prefer not to be informed, as that would just cause them unnecessary concern.

A number of participants felt that, even when a breach was not serious enough that the individuals whose data was possibly breached should be informed, some form of record of all breaches of personal information should be kept for purposes of collecting data that might help in identifying patterns, pinpointing areas where security could be improved or assisting law enforcement in fighting criminal data and identity theft. Some participants also felt that a record of all breaches would make it possible for authorities to determine whether any specific organizations were not taking sufficient security precautions and therefore experiencing more data breaches than would be expected if they were taking the appropriate precautions.

“At least for the statistical purposes, so that they know that there’s something or some activity going on. Or maybe this particular area is suddenly being targeted that we should be aware of.”

One participant in Calgary made the suggestion that there should be an independent organization responsible for receiving all reports of data breaches, and making this information available to individuals: “So at least we have the statistics on it, and on an individual case-by-case basis, giving us the choice of opting into the information or not; receive notification because I choose to receive notification.”

MAKING DECISIONS CONCERNING NOTIFICATION

When asked to consider who should in fact decide whether individuals should be notified about a particular breach, a few participants felt that the organization experiencing the breach should make the decision, because “they’re the ones who know what information of yours they have and what could be potentially dangerous if it got out.” However, most participants were concerned that any individual organization might have its own reasons to downplay the seriousness of a breach and that allowing them to make such decisions would involve a conflict of interest. These participants preferred that there be firm guidelines about when notifications should be made, and a legal requirement for notification under those guidelines.

“The government or people through the government create a law saying, when this particular type of information is breached, then notification should occur. ... self-policing and that is open to interpretation of the company, and quite honestly, someone might want to cover their own butt and say, ‘Oh, it was no big deal,’ when in fact it may be.”

Most participants felt that it was ultimately the responsibility of the government to protect people from the consequences of data breaches. As well, most agreed that decisions concerning notification were best made by a neutral “objective third party” – ideally a government-appointed review committee – that would not be influenced by concerns about customer perceptions, public image or the legal ramifications of a data breach. Other participants suggested that such decisions might be made by the Auditor General’s Office.

OFFICE OF THE PRIVACY COMMISSIONER

While some participants have heard of the federal Office of the Privacy Commissioner (OPC) or, in the Calgary groups, the Alberta Information and Privacy Commission (AIPC), most have only a vague idea of the activities and responsibilities of these bodies. Some associated the federal organization with the Freedom of Information and Protection of Privacy Act.

When asked to consider whether all data breaches should be reported to the OPC for a determination on whether the breach needs further action, most participants felt that it would be an appropriate body to handle such decisions. However, most also felt that clear guidelines should be

established to provide a framework for organizations reporting breaches and for the OPC’s decisions on notification and other actions.

“Well, they have to tell them certain things and they might come back and say, ‘Okay, this is something you have to tell your customers about.’ But there also should be a set line of, ‘Okay, your credit card was taken, you’re reporting that to the Privacy Commissioner but you automatically have to report that to your people.’ You don’t have to make a decision on that, that’s just set.”

Most participants expressed a preference for the federal OPC being the decision-making authority, rather than individual provincial privacy commissions; they argued that many of the organizations that might experience breaches, such as banks and financial institutions, and major retailers, operate in more than one province and their databases contain information on people across the country. Some also noted that having a federal body in charge of receiving reports and making decisions on notification would ensure uniformity of procedures and decision criteria. However, some participants – particularly in Montreal – felt that reports could be made to provincial commissions as long as there was a federal co-ordinating body that would oversee the activities of the provincial bodies, create a national database and act on a national level when appropriate.

While a few continued to feel that all breaches should result in notification of the affected individuals, most felt that an independent and neutral body such as the OPC could be trusted to determine when a data breach required notification. However, there was general support for the idea that all breaches should be reported and that a database of such incidents be maintained “for statistical analysis” and made accessible to the public: “even if I’m not notified, if somebody somewhere is being notified that there was a minor breach...” Some participants also favoured the idea that a “watch list” of organizations reporting frequent data breaches be published or otherwise made available for consumers to check.

FORM AND CONTENT OF DATA BREACH NOTIFICATIONS

In the event of a data breach involving their personal information, most participants would want to be notified by letter. A few felt that notification by e-mail would be acceptable, but others were concerned that e-mail notification might end up in a spam filter and not be read. There was little interest in notification by telephone. Participants had clear ideas about the kind of information that they would expect to find in such a notification. This included:

- What information was breached
- How the breach happened
- When the breach occurred
- How the breached information could be used
- What the organization is doing or plans to do to minimize the risk to those whose information has been compromised
- How the breach could affect the individual
- What action the individual should take to protect themselves from any consequences
- Name and contact information for a company representative.

For some, it was also important that the size and scope of the breach – how many people were affected – be included in any notification letter. Some thought that it would give them an idea of how likely it is that their information will be used in some way, while others said that just knowing their data had been breached will put them into “high alert mode.”

There was interest in the suggestion that when data breaches are reported to the Privacy Commissioner, the report would include how many people were involved, and the OPC would compile an annual report on the state of data breaches in Canada that would include the number of people affected by data breaches in that year.

Most participants agreed that if the breach took place when the data was in the possession of a third party acting on behalf of the organization that the individual gave their information to – retailer, employer, bank or financial institution – then notification should come from the organization that the data was initially given to, rather than a subcontracted organization such as a data processor or payroll service.

“...the company, like in the case of Winners, they can turn around and say, ‘No, we’re not doing business with XY Company anymore, we have switched to this and so forth because of the security breach problem.’ And they’re the ones who stand to lose. Because if you have a security breach at Winners, it doesn’t matter who processed it – you’re going to remember Winners.”

CONSEQUENCES FOR FAILURE TO REPORT DATA BREACH

Participants generally agreed that if notification of a data breach, either to individuals under specific situations or to an independent body such as the OPC, were required by law, then organizations should face significant penalties if they fail to make the required report. Most participants recommended fines, possibly associated with the number of individuals affected, as the penalty for failure to report.

In addition to heavy fines for the company, some participants suggested that the owners, officers or members of the Board of Directors of companies or organizations who fail to report a breach should be personally liable, and face either fines or jail sentences. These participants worried that, without personal liability, fines for failure to notify would simply become part of “the cost of doing business.”

It was also suggested that companies that fail to report might be required to accept ongoing oversight to determine whether further unreported breaches have occurred. There was also support for having the OPC conduct audits of an organization’s security practices, not just for organizations failing to report, but for any organization who requests assistance in improving their security.

PREVENTION OF DATA BREACHES

When asked to consider ways in which organizations might act to prevent or at least minimize the effects of data breaches, most participants were unable to offer any suggestions; they felt that to make suggestions concerning actions that could be done in the line of prevention would require technical expertise in the areas of computer and security systems that they lacked. However, there was agreement that organizations did have a responsibility to take all appropriate precautions, and that if a breach occurred in spite of their best efforts, they should be required to undertake a close examination of their information handling procedures in order to “close the loopholes” and minimize chances of the same thing happening again.

Most agreed that if standardization of security and information handling practices would help to prevent data breaches, then companies should be required to adopt such practices.

A few participants did suggest other actions, such as ensuring the physical security of both electronic and hard copy storage of personal information, and restricting the ability of employees to bring personal data storage devices (hard drives, thumb drives, etc.) onto the premises.

EFFECT OF DATA BREACH REPORTING ON CONSUMER LOYALTY

Most participants felt that being informed of a data breach would not necessarily mean that they would lose trust or confidence in the organization that had experienced the breach. In fact, some said they would be more likely to sever their relationship with an organization that had experienced a data breach and failed to inform the people affected by it.

Full and forthright disclosure accompanied by an indication of steps being taken to minimize the risk of further breaches might even result in some participants having a more positive view of the organization in question.

However, some did indicate that if an organization experienced ongoing data breaches without appearing to do anything to improve their security, or if the breach was the result of obvious negligence, then they would likely lose confidence. Some suggested that they might also lose confidence if the organization did not provide clear and useful information on how the individual should proceed in order to minimize their own risk.

“It depends on how they handle it when you talk to them. If they aren’t really going to be very helpful about it or give any suggestions or send you to the right people to get things straightened out, then you’re not going to want to stay with them.”

Participants also noted that if all organizations were obligated to report data breaches, this would in effect create a “level playing field” in which no company or organization would be at a disadvantage because they notified their customers or clients. In these circumstances, issues that might affect consumer loyalty would instead be the consumer’s perceptions of the seriousness with which the organization addressed the problem, and the respect and level of assistance offered to the customer or client.

CORPORATE AND INDIVIDUAL RESPONSIBILITY

While there was general agreement that both organizations and individuals had certain responsibilities with respect to data breaches of personal information, most participants tended to place the greater share of responsibility on the organization suffering the breach than on the individual whose data was compromised.

Participants did agree that once notified of a data breach involving their personal data, individuals had a responsibility to take whatever steps were available to them to minimize the effects of the breach. These steps might include checking financial statements, informing one's bank or credit card company that one's information had been compromised – and changing their accounts if advised to do so – checking one's credit rating, and changing passwords or access codes.

However, participants also agreed that corporate responsibility did not end with notification, and that notification did not erase liability. There was some difference of opinion, however, as to whether that responsibility might be lessened if the individual did not follow up on any recommended precautions. Some felt that even if individuals did not take these steps, the organization remained fully liable for any consequences to individuals whose data was breached; others thought that failure to follow such instructions would reduce the organization's liability.

“I can't see how it gives them a 'get out of jail free' card. I made a mistake; I'm telling you about it, okay, nobody can sue me for anything. That makes no sense.”

“I hate to say it, but if they've notified you and specifically told you, check your credit card statement or whatever, then the onus should be on you.”

Most agreed that the company or organization had a responsibility to take all necessary precautions to ensure that another data breach did not occur, including necessary security updates and changes to procedures.

As well, participants felt that the organization that experienced the breach should bear the cost of any steps that the individual might have to take, such as checks on their credit rating.

“If I have to go do something out of the norm in order to respond and protect myself because of something that happened within their jurisdiction, then yeah, I think they have some responsibility there.”

Some participants were asked about an individual’s responsibility to report a data breach if they happened to discover one. Most felt that the average person probably would not have the expertise necessary to identify any but the most obvious breaches, such as finding confidential documents in a public place, and that if they did discover such a breach, they would not be aware that they should inform the OPC. They did feel that most people, if they encountered something of that nature, would probably contact the organization if they were able to identify it, or inform the police. This was seen as a moral responsibility rather than a legal one.

There was some discussion of the OPC engaging in a public education campaign to provide people with information about data breaches in general and what they should do if they were affected by one, or discovered one.

Alberta Privacy Legislation

Participants in the Calgary sessions were asked to discuss various aspects of the recent legislation passed in the province concerning notification of data breaches.

Most participants in the Calgary sessions expressed limited awareness of the Alberta Information and Privacy Commissioner’s role with respect to data breaches: “We’ve heard about it, but that’s it.”

Participants were informed that the law says that if there is a data breach, the company has to notify the Office of the Information and Privacy Commissioner of Alberta without unreasonable delay, if the company thinks that a reasonable person would consider the breach to create real risk of significant harm.

Most participants felt that this legislation was too weak. Concerns were expressed that self-policing would lead to companies’ under-reporting due to conflict of interest: “Because the company could look at something and say, ‘Ah, that’s not so serious, let’s wipe that under the rug.’”

Further, participants felt that the standard by which a company was to determine whether it was required to report a specific breach was too vague and open to interpretation, which again opened up the possibility for a conflict of interest that might result in serious breaches going unreported. The phrases “reasonable person,” “real risk,” “significant harm” and “unreasonable delay” were seen as being not clearly defined, although some thought that there might be legal precedent for the idea of what a “reasonable person” would think, based on the idea of “reasonable doubt.”

Participants instead expressed a clear preference for having all breaches reported to the AIPC, who would then decide if notification of individuals was necessary.

While there was some acceptance of leaving the standard for deciding whether to notify an individual open to some interpretation as long as it was a neutral third party such as the AIPC doing the interpreting, participants felt strongly that a specific time period within which an organization had to make a report to the AIPC should be made part of the law. Most felt that a period of 24 to 48 hours after discovery of the breach was an appropriate time period.

Most felt that under the current law, it was unlikely that the AIPC would ever decide not to notify individuals about a data breach reported to them, given that the companies were only reporting breaches which they believed would pose a risk of significant harm.

“... let’s face it, a company would tend to under-report, so if they are going to report it, it’s already a big deal.”

When asked what they felt was the goal of the legislation, risk management or consumer protection, participants tended to say that the real goal of the law was primarily “window dressing” in that the government of Alberta was trying to make it appear that they were doing something about the problem of data breaches and how companies deal with them, but that in fact the law was relatively toothless and provided false confidence.

Participants were told that under the current law, if it is determined that a notification is necessary, the organization is required to include certain information in the notification, including: a description of the circumstances of the loss or unauthorized access or disclosure; the date or time period during which the data breach occurred; a description of the personal information involved in the loss; a description of any steps the organization has taken to reduce the risk of harm to

individuals; and contact information for a person who can answer on behalf of the organization questions about the loss.

Most felt that, in addition to these things, it was important for the company making the notification to provide the individual with advice on what steps they can take to reduce any chance of harm.

“You need to know how to follow up on your behalf. Or if there is nothing you can do, then you need to be assured there is nothing you can do.”

Suggestions on what kind of advice might be offered included:

- Check your statements
- Notify your credit card company
- Change your PIN codes or passwords
- Notify your bank
- Check your credit rating regularly.

APPENDIX A

September 14, 2010

Discussion Guide – Final (Calgary)
Environics Research
Attitudes towards data breach notification
PN 6717
Public Interest Advocacy Centre

1.0 Introduction to Procedures (10 minutes)

Welcome to the group. We want to hear your opinions. Not what you think other people think – but what you think!

Feel free to agree or disagree. Even if you are just one person among eight that takes a certain point of view, you could represent millions of Canadians who feel the same way as you do.

You don't have to direct all your comments to me; you can exchange ideas and arguments with each other too.

You are being taped and observed to help me write my report.

I may take some notes during the group to remind myself of things also.

The host/hostess will pay you your incentives at the end of the session.

Let's go around the table so that each of you can tell us your name and a little bit about yourself, such as what kind of work you do if you work outside the home and who lives with you in your house.

2.0 Awareness and experiences of data breaches (20 minutes)

Tonight we are going to be discussing issues around "data breaches." A data breach is *"the loss of, unauthorized access to or unauthorized disclosure of, personal information resulting from a breach of an organization's security safeguards."*

Have any of you heard of any data breaches recently in the news?

I want you to work together in pairs and spend a few minutes with your partner and create a list of what you currently know about data breaches and then I want you to make a list of what you most want to know about it and what your concerns are. Once

everyone has done that I want each team to report back to the group about what they came up with.

What do you know about data breaches? When you hear that there has been a “data breach” what does it mean?

IF NECESSARY: Here are some examples of data breaches – for example when:

- *An organization loses personal information – for example, an employee loses a laptop that contains personal information about clients,*
- *personal information in an organization’s custody or control is accessed in an unauthorized manner – for example, the organization’s client database is accessed by hackers or a point-of-sale terminal with stored credit and debit card information is stolen,*
- *personal information in an organization’s custody or control is disclosed in an unauthorized manner – for example, a “rogue” employee of the organization sells its customers’ credit card numbers to fraudsters.*

What do you most want to know about data breaches?

What kinds of organizations come to mind when you think of who could experience a data breach that could affect you?

PROBE: banks/financial institutions, credit card companies, phone companies, ISPs, large businesses with customer data bases and loyalty programs (i.e., airlines, etc.), government, etc.

What can be the consequences to individuals of a data breach?

PROBE: ID theft, loss of money, loss of personal information, inconvenience, etc.

Is it just about losing money or are there other consequences from a data breach (i.e., loss of privacy or release of confidential information)?

FOR GROUPS WITH DATA BREACH AND ID THEFT VICTIMS:

Have any of you ever personally experienced a data breach and/or identity theft? **IF**

YES: What happened?

How were you notified?

Did you lose money as a result?

Were there any non-monetary consequences? Were you inconvenienced at all?

ASK ALL

Do any of you know people who have experienced identity theft or were involved in a data breach? What happened?

As far as you know, when there is a data breach (i.e. at a financial institution, government, retail store, etc.) what has to happen? What obligations does the institution have, if any?

3.0 Conditions for notification of data breaches (20 minutes)

Are institutions obliged to notify customers or clients if there has been a data breach? Do people automatically get notified?

In fact, right now most provinces have no mandatory laws about notifying anyone that data breaches have occurred. There are some voluntary codes of conduct, but little that actually forces anyone to do anything. Alberta brought in a law just a few months ago and Ontario has a law that only deals with breaches of data on health information.

Data breaches of some sort happen quite frequently. In some cases they may be very minor (i.e. someone misplaces a laptop that contains lots of personal data for half an hour and then its recovered) and in some cases they could be much more serious and involve credit card information or financial information about a million people being breached and used illegally, etc.

If you were told of every single data breach of any kind at your bank or the government or businesses you deal with, etc., you might well be getting notified several times a year.

Do you think that consumers should be notified about ALL data breaches regardless of seriousness or is there a downside to this? Why? Why not?

There has been some discussion of having some sort of a “sensitivity test” around whether a data breach involves information that is “sensitive” enough to require notification. When someone talks about “sensitive personal information” what does that include? Can you each make a quick list of what personal information you think of as being “sensitive”?

PLEASE READ WHAT YOU EACH LISTED

PROBE IF NOT MENTIONED: Health information, financial/income information, personal ID such as SIN numbers or passport numbers, etc.

What about other kinds of data breaches that might not involve personal ID or financial information, what if it is things like your online address book and contact lists, chat histories, private social networking postings? Are those “sensitive”? Can these be sensitive? Do you consider your own information like this to be “sensitive”?

Does the circumstance of the breach matter? Does it matter if the information lost is that of a minor (teenager or child)?

What about information about your consumer behaviour and purchase patterns?

There has been a lot of discussion about having some guidelines for when institutions and companies should be legally obliged to notify their clients or customers that some sort of data breach has occurred. Are there certain types of data breaches involving certain kinds of information that should trigger notification?

PROBE IF NOT MENTIONED: what about social insurance number, drivers’ license number, health card number, credit card numbers, credit rating, date of birth and address?

What if the company or institution claims the information is “de-identified” or “anonymized” (for example it is encrypted) or somehow unusable by the thief or a finder? Should there still be a notification?

What if the company claims that the data breach was discovered in time had no consequences and that no one actually lost anything as a result?

4.0 Notifying authorities (10 minutes)

Who should decide if a data breach involves sensitive enough information to trigger notification? Can we trust the companies to decide or should it be a third party?

Should all data breaches have to be reported to a particular authority? Who should that be?

PROBE: the police? Credit bureaus? What about the privacy commissioner

How many of you have heard of the federal Privacy Commissioner? What about the Privacy Commissioner of Quebec? Do you know what its role is supposed to be?

What would you think of the idea of having all data breaches reported to the office of the privacy commissioner so that they can decide whether the breach needs further action? Would it make more sense of the federal Privacy Commissioner or the provincial Privacy commissioner to deal with data breaches?

Does it make sense that there be cases where data breaches would be reported to authorities such as the Privacy Commissioner and they may decide that in that case it's not necessary to notify each individual that the data breach occurred?

Should there be a public list or database of data breaches in Canada that people can look up?

5.0 Form of notification (10 minutes)

If you were notified of a data breach, what form should it take and what would you want to know?

Should there be any rules around what the notification should consist of? (e.g., there are a number of U.S. state laws spelling out what the notice should contain)

Should it describe in detail what data was lost? Should it tell you what to do next and who to contact if you have questions?

Should it provide a contact at the company for more information on the data breach?

Should it be in a standard format or should it vary for each company or government?

Who should the notice come from? The people who lost the information or the company for whom the information was being processed (e.g. a data breach at a company that does payments processing for a major retailer. Would you like to hear from the retailer, the data processor, or both)?

6.0 Client retention/customer loyalty (5 minutes)

If you got a notice about a data breach from a company you deal with, how would it affect your relationship with the company, if at all?

Would you immediately take your business elsewhere or would you give the company a “second chance”? What would it depend on? Would you expect help or some sort of compensation from the company?

7.0 Penalties for non-notification (5 minutes)

If a company had a data breach and didn’t report it when the law said they should, what should happen to them?

PROBE: Fined? Having to pay compensation to customers? Having to offer free credit monitoring to customers? Being audited for their security practices by someone like the privacy commissioner? Being liable to class action lawsuits?

8.0 Personal responsibility of consumers (5 minutes)

As a consumer, what is your responsibility, if any, if you have been notified of a data breach and you want to protect yourself from any losses?

Should consumers be required to take any steps after a data breach notification in order to be able to claim any compensation (for example, checking their credit report or checking for any unauthorized charges etc...)? In other words, if a consumer ignores a data breach notification, should they then be responsible for any losses they incur?

If the company notifies you of the data breach, have they done their part and they should be protected from any class action law suit?

9.0 Prevention (5 minutes)

Let’s move on to discussing what might be able to be done to prevent data breaches.

Should all companies and organizations be required to adopt a standard set of information handling processes to avoid data breaches in the future? If so, what steps could they take?

NB: These could include things like: (DO NOT READ)

- Secure user authentication protocols
- Secure access control measure
- Encryption of all transmitted records and files containing personal information that will travel across public networks and encryption of all data containing personal information to be transmitted wirelessly

- Reasonable monitoring of system for any unauthorized use of or access to personal information
- Encryption for all personal information stored on laptops or portable devices
- Up-to-date firewall protection and operating system security patches
- Up-to-date versions of system security agent software malware protection, patches, and virus definitions
- Education and training of employees on proper use of the computer system and the importance of personal information security

10.0 Alberta Law (Calgary only) – 10 minutes

There actually is a law in Alberta around disclosure of data breaches. Did any of you know about that?

It says that if there is a breach the company has to notify Office of the Information and Privacy Commissioner for Alberta (AIPC) if the **company** thinks there is a “Real risk of significant harm”. The company must assess if a “reasonable person” would consider the breach to create “real risk of significant” harm to individuals.

Are you comfortable with that test? What do you think that test really means/requires?

Do you think companies can place themselves in the position of a reasonable person when they are dealing with a breach from the company?

What do you think a "real risk" means? What do you think "significant harm" to an individual means?

After the AIPC is notified, the AIPC then decides if people should be notified. The AIPC has complete discretion on when to order notification and there are no criteria for this decision - though the AIPC gets complete info on the breach from the company. Can you think of any situation where a company might notify the AIPC of a breach that has a “real risk of significant harm” and the AIPC would NOT order notification under this test?

Companies and organizations that notify the AIPC of a breach must do so "without unreasonable delay". What do you think this means? Would it be better to specify an absolute limit to the time in which an organization must notify?

What is the goal of this law, risk management or consumer protection?

The content of the notice in Alberta requires:

- *a description of the circumstances of the loss or unauthorized access or disclosure;*
- *the date on which, or time period during which, the loss or unauthorized access or disclosure occurred;*
- *a description of the personal information involved in the loss or unauthorized access or disclosure;*
- *a description of any steps the organization has taken to reduce the risk of harm to individuals;*
- *contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure.*

Is this enough? Is something missing?

PROBE: number of others affected; what steps the organization has taken to notify individuals.

Should it have to provide advice on what steps to take to reduce the chance of harm suggested right in the notice?

Thanks for your participation!

APPENDIX B

August 9, 2010

**Environics Research Group Limited
Focus Groups on Attitudes towards data breaches
Public Interest Advocacy Centre
PN6717**

Recruitment for Group Discussion

Respondent Name: _____

Home #: _____

Business #: _____

Group #: _____

Recruiter: _____

GROUP 1

Montreal
Thursday, Sept. 9
5:30 pm
General Public

GROUP 3

Calgary
Wednesday, Sept. 15
5:30 pm
General Public

GROUP 2

Montreal
Thursday, Sept. 9
8:00 pm
Experienced data
breach/ID theft

GROUP 4

Calgary
Wednesday, Sept. 15
8:00 pm
Experienced data
breach/ID theft

Recruit 8 participants per group.

One session in each city to be with people who have been the victim of identity theft or who have been notified that there was a data breach where personal information of theirs may have

been breached and where there was the potential for them to have lost money or personal information. This would include mortgage fraud, credit card fraud, debit card fraud, identity theft etc...

“Identity theft (“ID theft”) is the unauthorized collection and fraudulent use of someone else’s personal information. Victims of ID theft can suffer financial loss, damage to their reputation, and emotional distress, and are left with the complicated and sometimes arduous task of clearing their names.”

The other session in each city will be with members of the general public who have NOT experienced any of these things. They must all be at least somewhat interested in public policy issues.

Hello, I'm _____ from Research House. We are telephoning to invite people to be a paid participant in a group discussion about some public policy issues in Canada.

- | | | |
|--------------|--------|---|
| 1. INDICATE: | Male | 1 |
| | Female | 2 |

NB: WE WILL GET A MIX OF MEN AND WOMEN IN EACH SESSION, BUT NO NEED FOR PARITY IN SESSIONS 2 AND 4 SINCE WE WANT TO FIND ANYONE WHO IS A VICTIM OF DATA BREACHES AND ID THEFT.

2. Do you, or does any member of your household, work for [READ LIST]?

- A market research company
- A government agency that regulates finance
- A bank or financial institution
- A credit card company

IF YES TO ANY, THANK AND TERMINATE. IF NO TO ALL, CONTINUE.

3. In general, how much attention do you pay to news about current events and public policy issues? **READ**

- | | |
|---------------------------|-----------------------|
| A great deal of attention | 01 - CONTINUE |
| Some attention | 02 - CONTINUE |
| A little attention | 03 - TERMINATE |
| No attention at all | 04 - TERMINATE |
| DK/NA | 99 - TERMINATE |

4. Thinking about the last five years, please tell me whether or not you personally experienced any of the following? **READ**

a. You were notified by your bank, financial institution or credit card company of a possible data breach on your account

Yes
No

b. You were the victim of “identity theft”

Yes (Please describe what happened) _____
No

c. You were the victim of a mortgage fraud

Yes (Please describe what happened) _____
No

d. Any other form of data breach (i.e. health records being breached, or account information with a company you do business with being breached etc...)?

Yes (SPECIFY) _____
No

FOR GROUPS 2 AND 4, ALL MUST SAY YES TO AT LEAST ONE OF THE ITEMS IN Q. 4, IF PERSON HAS NOT EXPERIENCED ANY OF THESE THINGS, THEY QUALIFY FOR GEN POP GROUPS 1 AND 3

IF YES TO ANY ITEMS IN Q. 4, ASK, Q. 5.

5. Thinking about your experience with [INSERT WHAT HAPPENED IN Q. 4], did you personally experience any financial loss, emotional distress or damage to your reputation?

Yes **TRY TO GET AT LEAST TWO PEOPLE IN EACH OF GROUPS 2 AND 4**
No

ASK ALL

6. Could you please tell me what is the last level of education that you completed?

- Some High School only.....1
- Completed High School.....2
- Trade School certificate.....3
- Some Post secondary.....4 **GET MIX**
- Completed Post secondary.....5
- Graduate degree.....6

7. We have been asked to speak to participants from all different ages. So that we may do this accurately, may I have your exact age please? _____. **WRITE IN**

- Under 20..... 1 **TERMINATE**
- 20-29 years of age..... 1
- 30-39 years of age..... 2
- 40-44 years of age..... 3 **GET MIX OF AGES**
- 45-54 years of age..... 4
- 54-70 years of age..... 5
- 71 years or more 6 **TERMINATE**

8. Are you working (CHECK QUOTAS)?

- Full Time (35 hrs. +) ()| 4 minimum
- Part Time (under 35 hrs.) () 2 max.
- Homemaker () 1 max.
- Student () 1 max.
- Retired () 1 max.
- Unemployed ()| 1 max.

9. What is your current occupation?

Type of Job	Type of Company
-------------	-----------------

IF MARRIED ASK: WHAT IS YOUR SPOUSE'S OCCUPATION?

Type of Job

Type of Company

10. Which of the following categories best corresponds to the total annual income, before taxes, of all members of your household, for 2009? **READ**

01 - Under \$30,000

02 - \$30,000 to \$60,000

03 - \$60,000 to \$80,000

GET A MIX OF INCOMES

04 - \$80,000 to \$100,000

05 - \$100,000 to \$150,000

06 - \$150,000 and over

99 - REFUSE/DK/NA

TERMINATE

11. Participants in group discussions are asked to voice their opinions and thoughts, how comfortable are you in voicing your opinions in front of others? Are you...(read list)

Very comfortable.....1- **MIN 5 PER GROUP**

Fairly comfortable...2

Not very comfortable.3|- **TERMINATE**

Very uncomfortable...4|- **TERMINATE**

12. Have you ever attended a focus group or a one-to-one discussion for which you have received a sum of money, here or elsewhere?

Yes 1

No 2 ---> **(SKIP TO Q.15)**

IF YES ASK:

13. When did you last attend one of these discussions?

(TERMINATE IF IN THE PAST 6 MONTHS)

14. How many focus groups or one-to-one discussions have you attended in the past 5 years?

(SPECIFY)

IF MORE THAN 5, TERMINATE.

15. Sometimes participants are also asked to write out their answers on a questionnaire. Is there any reason why you could not participate? If you need glasses to read, please remember to bring them. (Add hearing impairment.)

Yes.....1 - **TERMINATE**

No.....2

NOTE: TERMINATE IF RESPONDENT OFFERS ANY REASON SUCH AS SIGHT OR HEARING PROBLEM, A WRITTEN OR VERBAL LANGUAGE PROBLEM, A CONCERN WITH NOT BEING ABLE TO COMMUNICATE EFFECTIVELY.

INTERVIEWER TELL RESPONDENT

PLEASE BRING ALONG SOME FORM OF IDENTIFICATION AS YOU MAY BE ASKED TO SHOW IT.

IMPORTANT:

The session is 2 hours in length, but we are asking that all participants arrive 15 minutes prior to the start time of the session. Are you able to be at the research facility 15 minutes prior to the session time?

Yes.....1-**CONTINUE**

No.....2-**TERMINATE**

I would like to invite you to a group discussion on:

The session will last 2 hours in total and you will receive **\$75** to thank you for your participation.
location:

INTERVIEWERS:

Tell respondent that it is a small group and anyone who does not show or cancels at the last minute will compromise the project. Make sure they know we feel their opinions are valuable and we are serious about finding out what they have to offer.

NOTE:

PLEASE TELL ALL RESPONDENTS THAT THEY WILL RECEIVE A CONFIRMATION CALL THE DAY PRIOR TO THE SESSION. IF FOR SOME REASON THEY HAVE NOT HEARD FROM US THEY SHOULD CONTACT US AT _____. IF THEIR NAME IS NOT ON THE ATTENDANCE FORM THEY WILL NOT BE ADMITTED TO THE GROUP.