MeRC

McMaster eBusiness Research Centre

Consumer Identity Theft Prevention and Identity Fraud Detection Behaviours

by
John Gilbert and Norm Archer

McMaster eBusiness Research Centre (MeRC)

WORKING PAPER No. 38
March 2011

McMaster
University

CONSUMER IDENTITY THEFT PREVENTION AND IDENTITY FRAUD DETECTION BEHAVIOURS

By

John Gilbert and Norm Archer

MeRC Working Paper #38

March 2011

©McMaster eBusiness Research Centre (MeRC)

DeGroote School of Business

McMaster University

Hamilton, Ontario, L8S 4M4

Canada

gilbeja2@mcmaster.ca
archer@mcmaster.ca

ABSTRACT

Identity theft and fraud are crimes that have become prevalent in the 'wired world'. The financial consequences are significant and growing. Consumers may develop attitudes based on previous experience with identity theft and fraud. These attitudes affect the wide variety of behaviours consumers employ to prevent identity theft, detect identity fraud, and mitigate the impacts of identity fraud. Using survey data, this paper examines the relationship between past experience of consumers and their levels of concern, and derives the principal components that make up consumer behaviours. The components are physical prevention measures, account monitoring, agency monitoring, password security, and risky behaviour avoidance. These components were found to be almost orthogonal, implying that consumers tend to 'buy into' a particular component of behaviour, employing all the behaviours in that component without regard to other components. This can leave 'holes' in consumer defence against identity theft and fraud. Finally, the relationship between the levels of concern and these components of consumer behaviour are also examined.

Keywords: Identity theft, identity fraud, consumer concerns, principal component analysis, Canadian consumer behaviours

ACKNOWLEDGEMENT

This paper is based on data collected for a national survey of consumer identity theft by Susan Sproule and Norm Archer, available as MeRC Working Paper #23 “Measuring Identity Theft in Canada 2008 Consumer Survey”, July 2008 via http://merc.mcmaster.ca/working-papers/23.html. Financial support for this study came from the Natural Sciences and Engineering Research Council of Canada.

INTRODUCTION

The quintessential crimes of the information age are identity theft and the use of stolen identity to commit identity fraud. U.S. Secretary of Treasury John Snow called identity theft "the greatest threat to consumers today…" because it "...attacks the trust and confidence that nurture our open economy, even as it destroys individual lives" (Snow, 2003). According to a study by the U.S. Federal Trade Commission, 12% of Americans had been victims of some sort of identity theft over a 5 year period. In Canada, 6.5% of adults reported being victims of identity fraud in a single year. The out of pocket costs to Canadian victims amounted to $150 million, and 20 million hours to recover from the resulting damage (Sproule and Archer 2008b).

The responsibility for identity theft prevention can be said to fall on three groups: the consumers that provide the information, the organizations including businesses and governments that collect and use the information, and legislative bodies including national and regional governments that regulate the handling of personal information. The OECD (Organization for Economic Cooperation and Development) for example, emphasizes regulation and calls for the standardization of definitions and statistics, the enactment of legislation to provide legal remedies for the victims, and deterrence and enforcement for the perpetrators (OECD 2009). Example legislation includes the California Privacy Law (SB1386) and PIPEDA (Personal Information Protection and Electronic Documents Act) in Canada. On the other hand, the privacy commissioner for the province of Ontario stresses the importance of the role of organizations in protecting personal information, lists 15 cases of massive data breaches in organizations in just one year (2005) and calls for mandatory reporting of data breaches and greater use of physical controls and data encryption on the part of organizations (Cavoukian 2005). Despite all the efforts of legislators and organizations, the consumer, however, still has a vital role in protecting his or her personal data. Carelessness or lack of attention on the part of the consumer such as neglecting to protect passwords, disposing of identity information in regular trash, failing to secure regular mail or access to personal laptops, or responding to 'phishing' attacks, can undo all the preventative work of governments and business. These groups recognize this reality and have encouraged consumer education regarding identity theft and fraud. Sample education sites include the Federal Trade Commission's 'Fighting Back Against Identity Theft' and sample publications that include "Take Charge: Fighting Back Against Identity Theft" (FTC 2006), the "Consumer Identity Theft Kit" (Consumer Measures Committee 2007), "Identity Theft and You" (Office of the Privacy Commissioner of Canada 2009) and the "Reduce Your Roaming Risks" pamphlet (BMO 2006).

Identity cards have been suggested as a way to minimize some forms of identity fraud such as credit card fraud. In practice this has not been the case and the costs both in monetary terms and in the loss of privacy have outweighed the benefits (Jackson and Ligerwood 2006). Ultimately, biometric measures may make identity theft more difficult but in addition to current reliability and cost constraints, there are issues of universality, distinctiveness, permanence, collectability, performance, acceptability and resistance to circumvention that are inherent to various biometric technologies (Institute for Prospective Technological Studies 2005). Furthermore, these measures are not universal. Retrieving personal information from the trash (also known as dumpster diving) will not be prevented by biometric scanning at ATMs (Automated Teller Machines). Consumers now, and in the future, will still play a critical role in identity theft prevention and identity fraud detection. They need to be vigilant. Without a concerted program of customer education, legislation and technical solutions cannot prevent identity theft and fraud (Williams 2008). This paper examines the precursors and attitudes that relate to the behaviours that consumers employ to prevent and detect identity theft and fraud. Specifically, does past experience with identity theft and fraud relate to the level of concern about being a victim? And does the level of concern affect consumer behaviours?

The paper proceeds as follows. Section 2 defines identity theft and fraud, presents some background and introduces a high level model of consumer behaviour in preventing and detecting identity theft and fraud. Section 3 presents the method used to analyse the data in support of the model. Section 4 describes the results of the analysis in four parts; one for each of the components of the model. These are (1) the impact of previous experience on level of concern, (2) behavioural factors, (3) the level of concern as it relates to behaviours and (4) the change in level of concern as it relates to changes in behaviour. Sections 5 and 6 discuss the results and conclude the paper.

BACKGROUND

Identity theft is the unauthorized access to personal information or documents. On the other hand, identity fraud is a crime involving the use of false identity (Sproule and Archer 2007). Generally, most identity fraud relating to financial and credit accounts is broken down into two categories; existing account and new account fraud. Existing account fraud entails the illegal use of an existing account or credit relationship. There is some discussion as to whether credit card theft and subsequent fraud should be considered as identity crimes. The loss of a credit card is equivalent to the loss of cash since, in general, no personal information is obtained other than the customer's name and card number. In fact, in most cases, the loss of a credit card and its subsequent fraudulent use is more innocuous than the loss of cash. The card is usually replaced promptly and the customer is not usually responsible for any fraudulent use after reporting the loss of the card. Furthermore, the financial institutions that underwrite the losses feel they have adequate procedures in place to control this type of crime (Sproule and Archer 2008).

Despite the importance of the role of consumers, and significant survey work, there has been little analytical work done on the behaviour of consumers in their efforts to prevent, detect and mitigate the effects of identity theft and identity fraud. Kahn and Roberds (2007) developed a purely theoretical econometric model which predicts that identity fraud will exist in equilibrium, balancing the cost of increased fraud against the cost of increased conclusiveness in identification. Eisenstein (2008) constructed a model using parameters derived from surveys which accurately predicts the level of identity fraud but only for 'new account' fraud. Jamieson, Winchester and Smith (2007) proposed a model of enterprise fraud management. In addition to these 'macro' models, there are some 'micro' models that address specific aspects of consumer behaviour concerning identity theft such as personal information disclosure (Norberg, Horne and Horne 2007), the effects of privacy seals (Rifon LaRose and Choi 2005), and behaviour in the on-line environment (Milne, Labrecque and Cromer 2009, Milne, Rohm and Bahl 2004). There appear to be, however, no general theoretical models proposed for the behaviour of consumers in preventing and detecting identity theft and mitigating the effects of identity fraud.

This paper explores the relationships between consumer experience, attitude and behaviour in relation to identity theft and fraud. In particular, it investigates the kind of theft/fraud experienced in the past in relation to the level of concern and change in the level of concern about identity theft and the effects on the behaviours of consumers.[1] A high level diagram is shown in Figure 1.

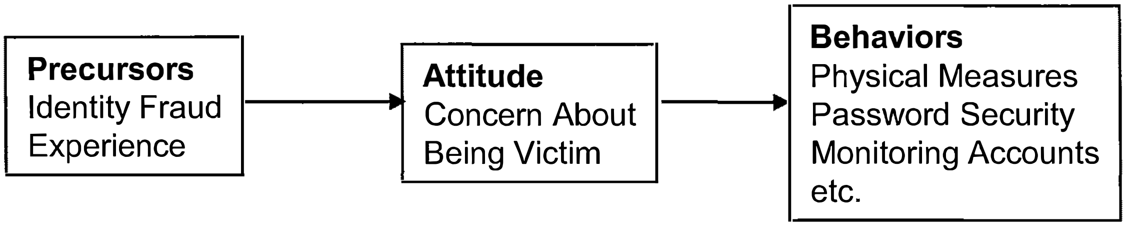

Figure 1 – Research Model

Given the financial and emotional costs of identity theft and fraud, one might expect that those who have experienced identity theft and fraud would have a different attitude and be more concerned with the possibility of being a victim of identity theft in the future. In particular, recent victims of identity theft and fraud may be expected to change their levels of concern. In keeping with the different characteristics of credit card fraud, the response in concern level could be at variance with those experiencing other identity fraud.

There are many behaviours that consumers exhibit in preventing and detecting identity theft and fraud. It is useful to group these behaviours using factor analysis. Few researchers, however, have done so. Milne, Labrecque and Cromer (2009) grouped 49 behaviours into protective and risky groupings. Their study, however, concerned only on-line behaviours and was directed as much at privacy and security as identity theft[2]. This paper will group 17 on-line and off-line identity theft and fraud prevention and mitigation behaviours into behavioural components. One might expect that the level of concern should have impacts on the behaviour components.

METHOD

The data for this paper come from the second study in the Identity Theft Program series sponsored by the Ontario Research Network for Electronic Commerce (ORNEC), conducted in 2008, by Sproule and Archer (Sproule and Archer 2008b). The program measures the nature and impact of identity fraud and identity theft in Canada. The survey was conducted by a professional marketing research firm. All respondents were required to be at least 18 years of age, reside in one of the 13 provinces or territories in Canada and have at least one bank account and one credit card. The sample was stratified based on age (5 categories), gender (50/50) and region (West, Ontario, Quebec and Atlantic). Demographic statistics are in Appendix B. When appropriate, responses were weighted, based on the population in each demographic strata (Appendix F). The survey was conducted in either English or French at the respondent's option. 3017 complete responses were obtained. An excerpt from the survey questionnaire, with all the

[1] This very loosely follows TRA, the Theory of Reasoned Action (Fishbein and Ajzen 1980). At a high level, TRA proposes that beliefs affect attitudes which precede intentions that in turn result in behaviours. With the data available in this study, behaviours are available and attitudes are operationalized as concerns over identity theft. Due to the limitations of the data collected, intentions and beliefs are unavailable. There are however, some data which may be antecedents of attitudes, i.e. past experience with identity theft and fraud.

[2] For example, one of the behaviours classified as risky was meeting someone in real life after meeting them first on-line.

items relevant to this paper, is included in Appendix A. The items used to operationalize precursors to consumer attitudes, the attitudes themselves, and the behaviours that consumers exhibited are outlined in Table 1.

Experience with identity theft and fraud which may be precursors to attitudes were surveyed in items 7, 8, 12, 13, 16, 17, 19, 20 and 44. Items 7 and 8 asked about credit card theft and fraud, 12 and 13 existing account fraud, 16 and 17 new account fraud, and 19 and 20 other identity fraud. Given the relatively small numbers of new account fraud and other identity fraud (1.1% and 1.5% respectively), these were grouped with existing account fraud respondents. The resulting data analysis was done with only two categories - credit card fraud and other identity fraud (existing account, new account and other identity fraud). The 3.7% of respondents who experienced both credit card and other fraud were counted as experiencing other fraud. Both groupings were split by respondents who had experienced fraud in the last year and those who had experienced fraud previously.

Item 44 concerned the subject of 'Phishing' attacks. Specifically it asked if the respondents had received emails from a bank or other company asking them to verify or update their account information in the last year. These experience items were studied as precursors to the development of a consumer attitude of concern towards identity theft and fraud.

Attitudes toward identity theft and fraud were surveyed in items 42 and 43. Item 42 asked about the current level of concern about becoming a victim. Item 43 asked about the current level of concern compared to one year previously. These items operationalized the attitude of concern towards identity theft and fraud.

Identity theft prevention, detection and mitigation behaviours were surveyed in four multi-part items. The first item (number 46) with 12 parts and second item (number 47) with 5 parts, assayed prevention and detection activities but with different scales. The third item (number 48) dealt with the use of pro-active risk management tools. The final behavioural item (number 49) with 5 parts, measured changes in behaviours.

Item 48 on the use of risk management tools posed some problems. In the three sub-items, the overwhelming percentage of respondents (90.0%, 90.3% and 86.0% respectively) had never used the risk management tool in question, which violated the normal distribution assumption.[3] Furthermore, the rest of the scale was problematic in that it had multiple interpretations. It was unclear if the consumer had started to use the tool more than 5 years ago and was still using it, if the correct response was 'more than 5 years' or 'in the last year'. The same applies to 'in the last 2 to 5 years'. For these reasons, item 48 was excluded from further analysis.

All responses to items 46 and 47 were recoded to numeric scales, with 1 being the most risk taking and the maximum of 5 being the least risk taking. This was also used to deal with reverse coded items such as using 'remember my password' where 'All of the time' was awarded a score of 1 (reverse coded to 5) etc. There were a total of 17 sub-items from items 46 and 47.

[3] Preliminary analysis showed that all three parts of question 48 loaded onto the same component probably due to the extremely skewed distribution.

The 17 sub-items in items 46 and 47 were used as inputs into a factor analysis of identity theft prevention and mitigation behaviours. Since the survey was conducted without a theoretical basis, no underlying latent variables were hypothesized. Principal component analysis was therefore considered the most appropriate technique to apply to behaviours. Since the sample was structured, all analysis was conducted by weighting each response according to the population weights given in Appendix F. The sample size of over 3,000 greatly exceeds the 1,000 recommended by Comrey and Lee (1992) for 'excellent' results from principal component analysis. It also exceeds 10 times the number of variables (17) with a minimum sample size of 200 suggested by Meyers et al. (2006).

The components identified were then used as dependent variables in an analysis with level of concern (item 42) as the independent variable. Since the concern scale (item 42) is ordinal but not interval, linear regression was judged inappropriate. A one-way multivariate analysis of variance (MANOVA) was therefore conducted to determine the relation between level of concern and the behavioural components.

Item 49, with 5 sub-items, surveyed changes to behaviour in the last year that might be motivated by a desire to reduce vulnerability. The relationship between changes in level in concern over the last year (item 43) and changes in behaviour (item 49) were analyzed with linear regression. To isolate demographic effects, the analysis was performed in two steps. The first step used the demographic items (age, gender and household income) as independent variables. The second used the demographic items and added the concern change (item 43) as an independent variable. Five such analyses were performed, one for each of the behavioural change items as dependent variable.

Table 1 Survey Items

Classification	Description	Time	Item	Scale
Attitude Precursors	Experienced Credit Card Fraud	Ever	7	yes no
		In Last Year	8	yes no
	Experienced Existing Account Fraud	Ever	12	yes no
		In Last Year	13	yes no
	Experienced New Account Fraud	Ever	16	yes no
		In Last Year	17	yes no
	Experienced Other Identity Fraud	Ever	19	yes no
		In Last Year	20	yes no
	Target of 'Phishing'	In Last Year	44	yes no

Attitude	Level of Concern About Being a Victim	Absolute	42	not at all slightly somewhat very extremely don’t know
		Change in Last Year	43	lower about the same higher don’t know
Behaviour	Prevention (12 sub-items)	Frequency	46	all of the time most of the time some of the time rarely never not applicable
	Monitoring (5 sub-items)	Frequency	47	Daily every few days every few weeks every few months yearly every 2-5 years every 5 or more years never not applicable
	Services Used (4 sub-items)	Frequency	48	Never more than 5 years ago in the last 2 to 5 years in last year not applicable
	Changed Activities (5 sub-items)	In Last Year	49	no change reduced stopped not applicable

Summarizing, the analysis was completed in four sets:
1. Relationship between identity theft and fraud experience, and level of concern about being a victim
2. Principal components analysis of identity theft and fraud prevention, and detection behaviours
3. Relationship between level of concern about being a victim, and identity theft and fraud prevention and detection behaviour components
4. Relationship between changes in the last year in level of concern about being a victim, and changes in the last year in behaviours that might expose the individual to identity theft or fraud.

Each set of analyses is documented in a separate sub-section in the following section.

RESULTS

The survey process delivered only complete responses so there were no missing data. The process also verified that all responses were valid. However, there were a number of items that allowed a 'not applicable' response (See Appendix B). Generally, on an item by item basis, the numbers of 'not applicable' responses were small and list wise deletion caused little loss of data. There were some exceptions in the prevention and detection items (46 and 47). These are discussed in the section on principal component analysis (Section 4.2)

A behavioural score was computed by summing the recoded responses to all items in items 46, 47, 48 and 49. The distribution of extreme behavioural scores was examined for outliers. The responses of the 5 lowest and highest scorers were examined individually to ensure that the respondents had not just automatically selected the same response for all items. Some of the items were reverse coded and the respondents had still selected the response that minimized or maximized the score so evidently they had at least read the question. The lowest score, however, was significantly below the second lowest score. In this case, the respondent had selected the extreme choice for all items on the survey including the non-behavioural items. This was judged to be not credible and this response was excluded from further analysis.

Descriptive statistics for all variables considered for analysis are given in Appendix C. Many violate the assumption of normality. In particular, Use Antivirus Software (item 46.5), Give Personal Info Over the Phone (46.9) and Check Land Registry (47.4) were highly skewed. Of the responses that were applicable (that is 'Not Applicable' was not selected), 77.8% always use antivirus software, 71.0% never give personal information over the phone and 77.6% have never checked the land registry.

Attitude – Concern About Being a Victim

The conjecture, that experience with identity fraud affects the level of concern, involves the items about experience of identity fraud (items 7, 8,12, 13, 16, 17, 19, and 20) and 'phishing' (item 37) and the items about the level of concern (item 42)[4] and change in level of concern (question 43)[5]. If the level of concern is treated as a linear scale[6], the relation is not evident from looking at mean concern levels as shown in Table 2. Chi-Square tests do, however, show differences at the .013 level of significance (Chi-square = 19.315, df=8). Figure 2 shows the percentage of the population at each level of concern for each fraud type experienced.

[4] Responses of 'don't know' were 0.6% for item 42 and have been excluded from this analysis.

[5] Responses of 'don't know' were 0.9% for item 43 and have been excluded from this analysis.

[6] 'Not at all' concerned was assigned a value of 1, 'slightly' 2 and so on to 'extremely' a value of 5.

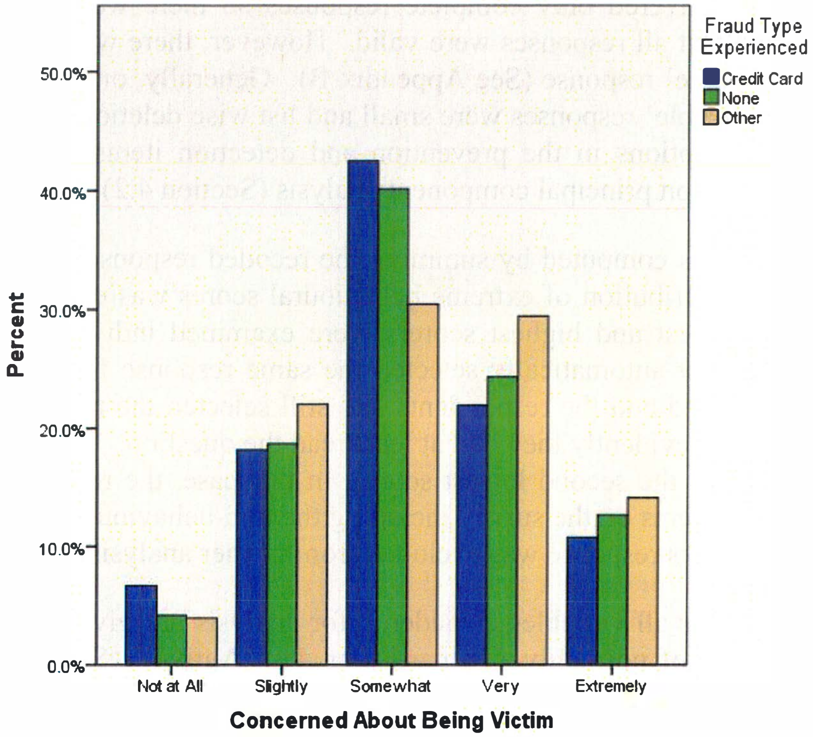

Figure 2 Concern Level by Fraud Type Experienced

Table 2 Concern Levels for Fraud Type Experienced

	Concern Level			
Fraud Type Experienced	Unweighted Count	Weighted Count	Mean	Standard Deviation
Credit Card	406	418.02	3.119	1.057
None	2,291	2,297.32	3.226	1.028
Other	301	281.35	3.278	1.043

While the mean concern levels for each type of fraud experience are almost identical, the distributions are not. Perhaps the most unexpected finding is that the percentage of respondents with no experience of identity fraud are always between the percentage of respondents that experienced credit card fraud and those that experienced other identity fraud.

Looking at whether the recent experience of identity fraud has differing effects, and treating the concern level as a linear scale, yields the results in Table 3 where 'lately' implies 'in the last year'. Chi-Square tests show differences at the .007 level of significance (Chi-square = 33.212, df=16). Figure 3 shows the percentage of the population for each level of concern for each fraud type experienced in the last year and before.

Table 3 Concern Levels for Timing of Fraud Type Experienced

	Concern Level			
Fraud Type Experienced	Unweighted Count	Count	Mean	Standard Deviation
Credit Card	295	314.94	3.197	1.078
Credit Card “Lately”	111	103.08	2.880	0.970
None	2,291	2,297.32	3.226	1.028
Other	209	194.43	3.360	1.016
Other “Lately”	92	86.93	3.096	1.089

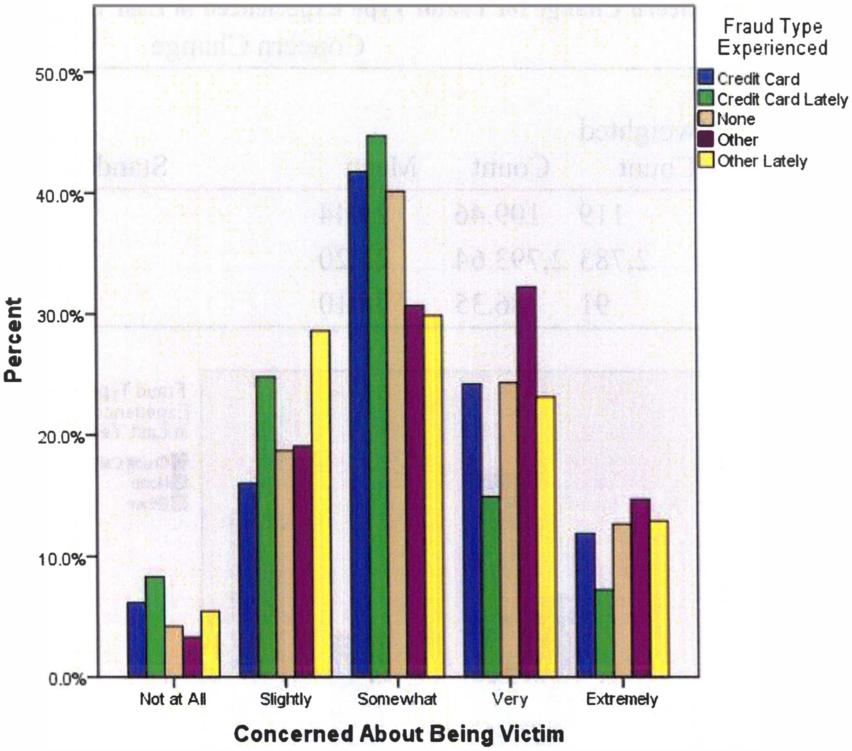

Figure 3 Concern Level for Timing by Fraud Type Experienced

Respondents who experienced identity fraud in the last year, whether credit card or other identity fraud, were less concerned about becoming a victim than those who had experienced the same fraud type previously. Only 22.2% of respondents who experienced credit card fraud in the last year were very or extremely concerned with becoming a victim, compared with 36.1% who had experienced credit card fraud previously. This latter is almost the same as those that had never experienced identity fraud at 37.0%. 36.1% of those respondents who experienced other identity fraud in the last year were very or extremely concerned with becoming a victim compared with 46.9% who had experienced other identity fraud previously.

Change in level of concern over the last year was surveyed in item 43. Treating the change in level as a linear scale by type of identity fraud experience in the last year yields the results in Table 4. Chi-Square tests show differences at the .001 level of significance (Chi-square = 37.471, df=4). Figure 4 shows the percentage of the population for each change of concern level, for each fraud type experienced in the last year.

Table 4 Concern Change for Fraud Type Experienced in Last Year

	Concern Change			
Fraud Type Experienced in the Last Year	Unweighted Count	Count	Mean	Standard Deviation
Credit Card	119	109.46	2.444	0.517
None	2,783	2,793.64	2.320	0.492
Other	91	86.35	2.610	0.478

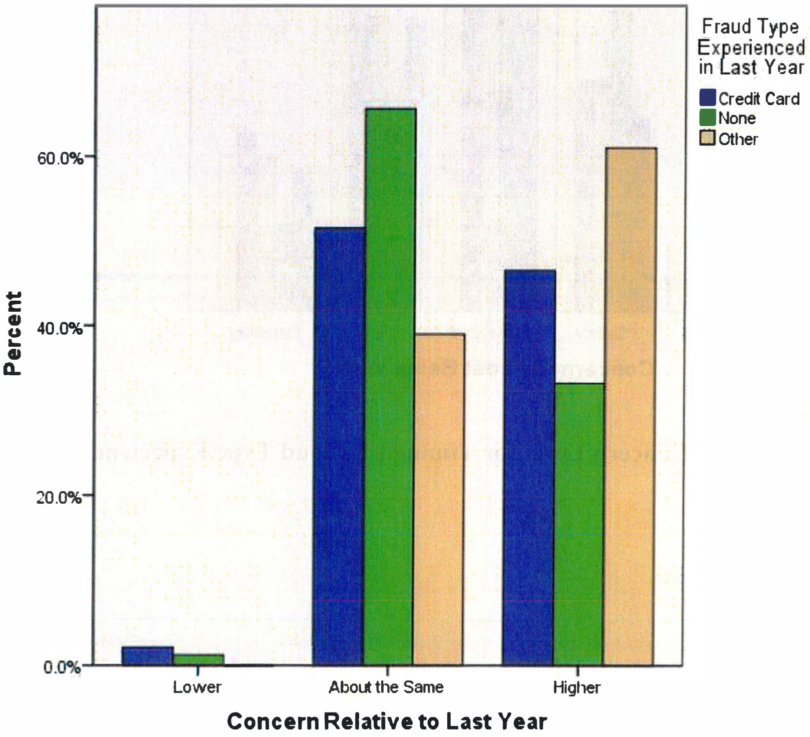

Figure 4 Concern Level Change for Fraud Types Experienced in the Last Year

The impact of identity fraud other than credit card fraud in the last year on the change in level of concern is considerable. Of those respondents that reported being the victim of other identity fraud in the last year, 61% judged their concern as higher, while none said it was lower. Contrary to absolute levels of concern, the respondents that reported being the victims of credit card fraud in the last year were intermediate between the percentage of those that experienced other identity fraud and those that experienced no identity fraud in the last year.

'Phishing' attacks were the subject of item 44. Specifically the question asked was, had the respondents received emails purportedly from a bank or other company asking them to verify or update their account information in the last year. Treating the change in concern level as a linear scale yields the results in Table 5. Chi-Square tests show differences at the .001 level of significance (Chi-square = 39.128, df=2). Figure 5 shows the percentage of the population for each change of concern level for respondents subject to 'phishing' attacks in the last year.

Table 5 Concern Change for 'Phishing' Attack Experienced in Last Year

	Concern Change			
'Phishing' in Last Year	Unweighted Count	Count	Mean	Standard Deviation
Yes	1,270	1,242.42	2.398	.512
No	1,723	1,747.02	2.287	.479

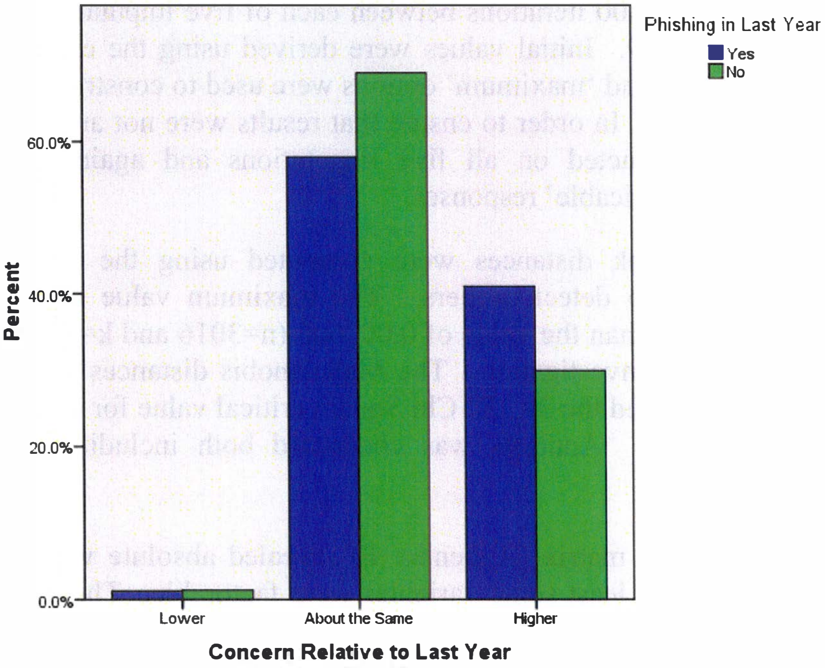

Figure 5 Concern Level Change for 'Phishing' Attack Experienced in the Last Year

The portion of respondents reporting higher levels of concern was greater if they had been subject to 'phishing' attacks in the last year than if they had not.

A linear regression of concern level on identity fraud experience and demographic variables (age, gender and household income) yielded significance at the .05 level or better for only age and identity fraud experience, and a miniscule effect size (R^2 = .030). In a regression of concern change on the same variables, only age and identity fraud experience again were significant at the .05 level and the effect size was even smaller (R^2 = .020). The impact of these control variables can therefore be ignored.

Principal Component Analysis of Behaviours

As noted earlier, there were significant numbers of 'not applicable' responses in items 46 and 47. Listwise deletion of these cases would reduce the sample to about half but more critically would bias the sample. By far the two largest cases of 'not applicable' responses were to the sub-items of educating children about not disclosing personal information (39.8%) and checking the land registry (25.5%). Leaving out these responses would bias the sample to include only home owners with children of teachable age. It was decided that the sub-item, educating children (46.10) would be dropped from analysis. This is defensible on theoretical was well as practical grounds. All of the other behaviours surveyed in items 46 through 49 (25 in all) addressed personal protection. The 'educate children' question is at variance with these behaviours in that it solicits information about a behaviour designed to influence others rather than protect oneself. Dropping the sub-item also significantly alleviates the 'not applicable' problem. 1,877 responses or 62.2% had no 'not applicable' values in the remaining 16 sub-items analyzed in items 46 and 47. 2,899 or 96.1% had 2 or fewer 'not applicable' responses. The analysis was conducted using imputed values for 'not applicable' responses. Imputation was performed by the Multiple Imputation procedure of SAS version 9 using a single Markov Chain Monte Carlo method with 200 'burn in' iterations and 100 iterations between each of five imputations. Input was all sub-items in items 46, 47 and 49. Initial values were derived using the expectation-maximization algorithm. The 'minimum' and 'maximum' options were used to constrain the imputed values to the range of valid responses. In order to ensure that results were not artefacts of the imputation process, analysis was conducted on all five imputations and again using only the 1,877 respondents with no 'not applicable' responses.

Both Mahalanobis and Cook distances were computed using the sub-items in items 46, (excluding 46.10) and 47 to detect outliers. The maximum value of Cook's distance was 0.00224 which is much less than the value of 0.007606 (n=3016 and k=1) specified by Kim and Storer (1996) as worthy of investigation. The Mahalanobis distances were more problematic. 106 responses (3.5%) exceeded the 39.252 Chi Square critical value for 16 degrees of freedom at the 0.001 confidence level. Analysis was conducted both including and excluding these responses.

Inspection of the correlation matrix (Appendix E) revealed absolute values in the range from .006 to.608 indicating that at least some variables were factorable. The determinant was 0.117 which is much greater than the 0.00001 value that would indicate problems of mulitcollinearity. Given the large sample size, Bartlett's test of sphericity was significant at the 0.0001 level. The Kaiser-Meyer-Olkin measure of sampling adequacy for factor analysis was 0.777 which comfortably exceeds the heuristic of 0.70 (Kaiser 1970, 1974).

Table 6 Communalities

46.1 Use Locked Mailbox	0.4542
46.2 Shred Documents	0.4653
46.3 Locked Financial Information	0.5660
46.4 No One Watches at ATM	0.4987
46.5 Use Antivirus Software	0.3272
46.6 Use Remember Password	0.3908
46.7 Use Different Passwords	0.6010
46.8 Use Hard-to-break Passwords	0.5028
46.9 Give Personal Info Over Phone	0.4976
46.11 Click on e-mail Link	0.4678
46.12 Approximate Balance Compare at ATM	0.5215
47.1 Monitor Bank Balance	0.7799
47.2 Monitor Credit Card	0.7334
47.3 Get Credit Report	0.6176
47.4 Check Land Registry	0.6307
47.5 Change Passwords	0.5305

Communalities are shown in Table 6. Use Antivirus Software (46.5) and Use Remember Password (item 46.6) were fairly low at .3272 and .3908 respectively.

The survey was conducted with no a priori theory. There were no hypotheses about factors or latent variables. Principal component analysis is therefore appropriate. Using the 16 sub-items (excluding the 'educate children' sub-item) in questions 46 and 47 yielded the initial Eigen values as shown in Table 7 and plotted in figure 6. Using the Kaiser-Guttman criterion of retaining factors with Eigen values greater than 1 gives a 5 component solution accounting for 53.7% of the total variance. Looking at the 'scree' plot in figure 1, a case could be made for using 3, 4, 5 or 6 components. Extracts and both varimax (orthogonal) and oblimin (oblique) rotations were performed, selecting 3 through 6 components. The 5 component solution was cleanest denoting strong loadings on primary components, weak cross-loading components and meaningful components.

Table 7 Initial Eigen values

Component	Total	% of Variance	Cumulative %
1	3.216	20.100	20.100
2	1.681	10.505	30.604
3	1.415	8.841	39.445
4	1.213	7.581	47.026
5	1.061	6.630	53.656

6	.915	5.721	59.378
7	.879	5.496	64.873
8	.864	5.400	70.274
9	.778	4.864	75.137
10	.707	4.416	79.553
11	.637	3.981	83.534
12	.618	3.864	87.397
13	.586	3.660	91.057
14	.537	3.356	94.413
15	.523	3.269	97.681
16	.371	2.319	100.000

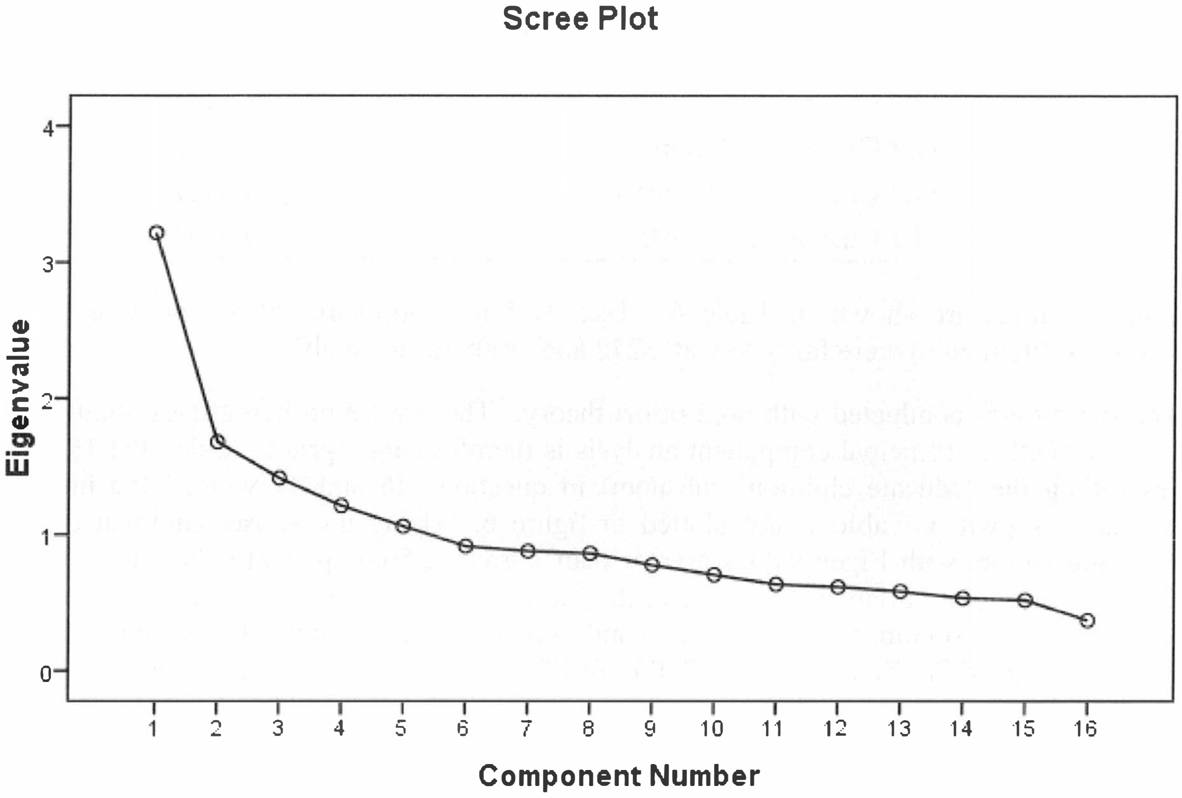

Figure 6 Scree plot of the Eigen values for the Principal Components Analysis

There were only three cases where a given sub-item loaded at an absolute value more than 0.3 on a ‘foreign’ component and/or had loaded at an absolute value less than 0.5 on its ‘own’ component for the orthogonal rotation. (The same patterns held in the oblique rotation.) In order to ensure a ‘clean’ loading those 3 sub-items 46.5 (I use anti-virus, anti-spyware and firewall software that is up-to-date on my computer), 46.12 (I know the approximate balance of my account to compare to the balance shown when withdrawing cash at an Automated Banking Machine) and 47.5 (I change important passwords i.e. for online banking, email accounts, etc.) were dropped. Principal component analysis on the remaining 13 sub-items revealed another one with weak loading on its own component and relatively strong loading on other components. Sub-item 46.4 (I make sure no one is watching when using an automated banking machine (ABM) or debit machine at a checkout counter.) was also dropped.

The 5 component solution for the 12 retained sub-items was almost orthogonal as shown in the component correlation matrix from the oblimin oblique rotation in Table 8. As expected, given the factor correlation matrix, the oblique rotation differed little from the orthogonal rotation. The oblique rotation offered marginally higher loadings and lower loadings on 'foreign' components, however, and was selected as the best solution.

Table 8 Component Correlation Matrix

Component	1	2	3	4	5
1	1.00000				
2	0.20456	1.00000			
3	0.13066	0.12999	1.00000		
4	0.08749	0.12388	0.17631	1.00000	
5	0.03722	-0.07130	0.10739	0.06674	1.00000

The final rotated structure matrix with the remaining 12 sub-items using imputation 1 is shown in Table 9. The highest loadings were the monitoring of bank balances and credit cards at .893 and .843 respectively. All of the components had multiple items that loaded at a value of 0.6 or greater. While these are not particularly high relative to items on standardized instruments, they are reasonably strong given the nature of the survey, the relatively low loadings on 'foreign' components and the departures from normality displayed by some of the items. Furthermore they compare favourably to the characterizations of good (.55), very good (.63) and excellent (.7) as specified by Comrey and Lee (1992). The maximum absolute value loading on 'foreign' components was .25 with all but 5 under 0.1.

The first component, items 47.1 and 47.2, accounted for 12.6% of the total variance and can be interpreted as monitoring account activities. Monitoring agencies makes up component 2 with items 47.4 and 47.3 and accounts for 11.5% of the variance. It should be noted that both items were highly skewed with 48.5% of respondents having never gotten a credit report and 58.2% having never checked the land registry. This latter statistic is of some concern in the light of the 24.7% for whom checking the land registry was not applicable. In other words, 77.4% of those for which the land registry item was applicable, had never check the land registry. Component 3, accounting for 11.1% of the variance, includes the behaviours related to password security; items 46.7 and 46.8. Component 4, which can be interpreted as physical prevention measures, includes items 46.1, 46.2 and 46.3, accounts for 11.3% of the variance. The final component, items 46.9, 46.11 and 46.6, can be interpreted as avoiding risky behaviours and accounts for 10.8% of the variance. Note that component 5 includes all 3 reverse coded items and, as already noted, the distribution of item 46.9 was highly skewed. These issues may have caused the loading for this component. (See Table 10. for % variance explained) The pattern matrix had similar loadings on the same factors.

Table 9 Oblique Rotated Structure Matrix

Item	Component 1	2	3	4	5
47.1 Monitor Bank Balance	**0.89283**	-0.06732	-0.01348	0.00916	-0.01526
47.2 Monitor Credit Card	**0.84312**	0.08156	0.01557	0.00477	0.01424
47.4 Check Land Registry	-0.01996	**0.82075**	0.02967	-0.03218	-0.02768
47.3 Get Credit Report	0.03769	**0.80625**	-0.00254	0.01761	0.03117
46.7 Use Different Passwords	0.02870	0.03687	**0.77470**	-0.03275	-0.03192
46.8 Use Hard-to-break Passwords	0.00719	0.01925	**0.72883**	0.07806	0.04447
46.1 Use Locked Mailbox	0.02913	0.02604	-0.25465	**0.73236**	-0.01236
46.2 Shred Documents	-0.00401	-0.12634	0.24632	**0.63161**	0.03745
46.3 Locked Financial Information	0.02088	0.14543	0.24904	**0.61536**	0.00470
46.9 Give Personal Info Over Phone	-0.02366	0.04432	0.03555	0.07349	**0.67914**
46.11 Click on e-mail Link	0.05255	-0.05824	0.07657	-0.14504	**0.66432**
46.6 Use Remember Password	-0.02129	0.00907	-0.10003	0.05117	**0.62055**

Table 10 Total Variance Explained

Component	Total Eigen value	% of Variance	Cumulative %
1 Account Monitoring	1.516	12.63	12.63
2 Agency Monitoring	1.380	11.50	24.13
3 Passwords Security	1.337	11.14	35.27
4 Physical Prevention Measures	1.352	11.26	46.54
5 Risky Behaviour Avoidance	1.294	10.79	57.32

The results of the analysis on the other 4 imputations were similar. All items loaded onto the same factors in each case. Comparison of the loadings from imputation 1 with 2 through 5 revealed a maximum difference of .067 with the vast majority under .02.

Principal component analysis using the original (not imputed) data is shown in Appendix G. There were no material differences from the imputed data, with the same sub-items loading on the same factors with close to the same weights. The differences between the non-imputed and the imputed results were similar to the differences between the various imputations.

The principal components analysis was also repeated without the 106 responses for which the Mahalanobis value exceeded 39.252 (Chi Square df=16, p<.001). The resulting 5 component solution accounted for 62% of the total variance. The rotated component pattern and structural matrices had no significant differences with all items loading onto the same components as before (See Appendix H).

Behaviours as Dependent on Concern

A one-way multivariate analysis of variance (MANOVA) was conducted on the principal components of behaviour. The independent variable was the concern about being a victim (item 42).

Scores for each component were computed by adding the values of each sub-item identified as contributing to the component. The sub-items in item 47 were linearly transformed to conform to the scale used in item 46 (i.e. 1 to 5) before addition. Each score was then divided by the number of sub-items in it to create scores that all had the same scale.

As with the principal component analysis, in order not to bias the analysis, imputation was used to fill in ‘not applicable’ responses. A statistically significant Box’s M test ($p<.001$) indicated heterogeneous variance across levels of concern, necessitating the use of Pillai’s trace to assess the multivariate effect. Using Pillai’s trace, the behavioural components were significantly affected by the level of concern about being a victim of identity theft and fraud (Pillai’s trace = .029, $F(20, 12880) = 4.632$, $p < .0001$, $\eta^2 = .007$). Univariate analysis (Table 11) indicated that all components except avoiding risky behaviours were significantly affected by level of concern. The variance accounted for, as evidenced by the values of η^2 however, is very small.

Table 11 – Univariate Analysis of Variance for Level of Concern

Dependent Variable	Df	F*	Sig.	η^2
1 – Monitor Accounts	4	3.848	.004	.005
2 – Monitor Agencies	4	3.899	.004	.005
3 – Password Security	4	4.540	.001	.006
4 – Physical Security	4	15.050	.000	.018
5 – Risky Behaviours	4	1.396	.233	.002

Tamhane post hoc tests, appropriate because of the heterogeneous variance, were conducted on the significant dependent variables, components 1 through 4. The results are shown in Table 12. Significant differences were between the extremely concerned level and the somewhat concerned levels for the monitor accounts component. For the monitoring agencies component, significant differences were found between the extremely concerned level and the slightly and somewhat concerned levels. The same pattern of significant differences applied to the password security component. The physical security component had the most number of significant differences with both extremely and very concerned level showing significant differences with the slightly and somewhat concerned levels and the somewhat concerned level showing a significant difference with the slightly concerned level. Of note, there were no statistically significant differences between the 'not at all' and 'extremely' concerned levels for any of the behavioural components.

Table 12 Tamhane Multiple Comparisons

Dependent Variable	Concern Level	Not at All	Slightly	Somewhat	Very	Extremely
1 – Monitor Accounts	Slightly	-0.0262	0.000			
		1.000				
	Somewhat	0.0107	0.0369	0.000		
		1.000	.542			
	Very	-0.0268	-0.0006	-0.0375	0.000	
		1.000	1.000	.511		
	Extremely	-0.0867	-0.0605	-0.0974	-0.0599	0.000
		.745	1.000	.000*	.167	
2 - Monitor Agencies	Slightly	0.1498	0.000			
		.644				
	Somewhat	0.1141	-0.0357	0.000		
		.882	.989			
	Very	0.1074	-0.0424	-0.0067		
		.925	.979	1.000	0.000	
	Extremely	-0.0358	-0.1856	-0.1499	-0.1432	0.000
		1.000	.009*	.032*	.073	
3 – Password Security	Slightly	0.1131	0.0000			
		.926				
	Somewhat	0.0421	-0.0710	0.0000		
		1.000	.737			
	Very	-0.0125	-0.1256	-0.0546	0.0000	
		1.000	.123	.870		
	Extremely	-0.1279	-0.2410	-0.1700	-0.1153	0.0000
		.881	.001*	.017*	.371	
4 – Physical Security	Slightly	0.2051	0.0000			
		.483				
	Somewhat	0.0006	-0.2045	0.0000		
		1.000	.002*			
	Very	-0.1512	-0.3563	-0.1518	0.0000	
		.822	.000*	.012*		
	Extremely	-0.2513	-0.4564	-0.2519	-0.1001	0.0000
		.223	.000*	.000*	.644	

Top number is mean difference
Bottom number is significance
* Significance at the .05 level or better

Change in Behaviour as Dependent on Change in Concern

Item 49 surveyed the changes in behaviours related to preventing identity theft including online shopping (49.1), receiving paper statements (49.2), handing a credit card to an attendant (49.3), carrying unnecessary documents (49.4) and banking online (49.5). A two step linear regression analysis was conducted with each of the sub-items as dependent variable. The first step controlled for demographic variables. The demographic independent variables in the first step were age, gender and household income. The second step added the change in level of concern as an additional independent variable. Summary results are displayed in Table 13.

In all cases, concern change was significant at the .0001 level with the exception of banking online which was significant at the .05 level. The effects are very small, however, with the contribution of change in concern accounting for explanation of variance ranging from 0.2% for online banking to 2.2% for shopping online.

Table 13 Linear Regression Results of Change in Behaviour Depending on Change in Concern

		R^2 Change	Sig. Change
Stepl – Demographics	49.1 Shopping Online	.040	.0001
	49.2 Receiving Paper Statements	.005	.013
	49.3 Handing Card to Attendants	.061	.0001
	49.4 Carry Unnecessary Documents	.026	.0001
	49.5 Banking Online	.020	.0001
Step2 – Addition of Concern Change	49.1 Shopping Online	.022	.0001
	49.2 Receiving Paper Statements	.008	.0001
	49.3 Handing Card to Attendants	.016	.0001
	49.4 Carry Unnecessary Documents	.013	.0001
	49.5 Banking Online	.002	.042

DISCUSSION

The difference in concern level by those that experienced credit card theft and fraud from those that experienced new account, existing account and other identity theft and fraud indicates that, in the view of consumers, credit card crime is distinct. This is probably due to the fact that credit card companies, and not consumers, take the risk for credit card fraud, provided that consumers notify their credit card issuers when credit cards are stolen, lost, or unauthorized payments are detected in the accounts (Barker, D'Amato & Sheridon, 2008). Indeed, the finding that consumers that have never been a victim of identity theft are intermediate in level between the consumers that have been victims of credit card fraud and those that have been victims of other identity fraud, indicates the differences in attitudes of the two groups that have been victimized.
The effect of the timing of the experience of identity theft on the level of concern is somewhat surprising. When respondents were victims in the most recent year, whether it was credit card or other fraud, their concern levels were lower than those who were victims previously. On the other hand, a large number of victims in the most recent year reported their concern level was higher than the previous year. The implication of these two findings is that victims of identity theft and fraud in the most recent year had previously very low levels of concern. This suggests that consumers with low levels of concern about identity theft and fraud are more likely to be victims.

The 5 component solution to the principal component analysis produces a fairly logical categorization of identity theft prevention behaviours. The final components of physical security, password security, avoidance of risky behaviours and monitoring of accounts and agencies make intuitive sense. It is remarkable perhaps that the items loaded so cleanly. There is no reason other than general vigilance, for example, to expect that someone who shreds confidential documents would also use a locked mailbox.

Conceivably, the most surprising finding in the principal component analysis is that the components are almost orthogonal. The correlations between most components are quite low. For example, individuals who monitor their bank accounts and credit cards do not necessarily also employ physical security (correlation=0.08749) or avoid risky behaviours (correlation=0.03722). It appears as if individuals 'buy into' a form of identity theft protection and employ all the behaviours associated with that form without reference to other forms. Consumers act selectively in the types of behaviours they employ and do not seem to embrace all forms of identity theft prevention and detection.

This selectivity can have significant consequences for consumers. The 2005 identity fraud survey (Javelin Research 2006) found that victims who detected the crime by monitoring accounts online, "experienced an average financial loss of $551" compared "with an average loss of $4543 when the crime was detected through paper statements". Consumers need to be encouraged to employ all forms of defensive and detection behaviours if identity theft is to be avoided and if costs are to be minimized when identity fraud does occur.

The effect of level of concern on identity theft and fraud prevention and mitigation behaviours is statistically significant but small. The reason is suggested by the fact that the behaviours of those who are not at all concerned about being a victim are statistically the same as those that are extremely concerned. Those who take identity theft and fraud very seriously may employ measures that they believe protect them from victimization. They may thus be 'not at all' concerned about being a victim. Concern may thus be moderated by the perceived effectiveness of behaviours intended to prevent identity theft. Rather than concern, perhaps a better attitude to measure would be the perceived prevalence or seriousness of identity theft.

Similar results were obtained for changes in behaviour. While change in concern had statistically significant effects on the change in all behaviours surveyed, the effect was small. Again, the change in concern may have resulted from the perceived effects of a change in behaviour.

CONCLUSION

Identity theft and fraud are wide spread and have significant financial impacts both in the costs of prevention and the costs of fraud when prevention fails. In addition, there are emotional and psychological impacts on victims. While businesses and governments have significant roles to play in minimizing the occurrence and consequences of identity theft and fraud, a critical role remains for consumers.

While concern about being a victim of identity theft and fraud is influenced by and in turn influences consumer behaviours, the relationships are not strong or linear. Other attitudes may be more effective in explaining consumer behaviour.

From the principal component analysis of the survey, it appears that individuals in Canada employ 5 main forms of identity theft protection and detection: physical security, password security, avoidance of risky behaviours, account monitoring and agency monitoring. The use of these forms are not correlated, however. Individuals appear to 'buy into' each form as a block and tend to employ all the behaviours associated with the form and only engage in other behaviours if they 'buy into' another form. Failure by consumers to employ all defensive and mitigation behaviours leaves 'holes' which thieves and fraudsters can exploit. Whether these patterns of behaviour are present in other countries, remains a question for further research.

The contribution of this research is largely the identification of the principal components of consumer behaviour that is intended to reduce exposure to identity theft and fraud. The finding that the components are almost orthogonal adds a new dimension to the understanding of the ways consumers handle the threat of these offences. For practitioners, this highlights the need to educate consumers in the necessity of employing all forms of identity theft protection. This research also fills, although without great effect, a 'hole' in models between the 'macro' models that explain the overall functioning of identity theft and fraud (Eisenstein 2008, Jamieson, Winchester and Smith 2007) and 'micro' models that concentrate on specific aspects of identity theft such as personal information disclosure (Norberg, Horne and Horne 2007), the effects of privacy seals (Rifon LaRose and Choi 2005), and consumer behaviour in on-line environments (Milne, Labrecque and Cromer 2009, Milne, Rohm and Bahl 2004)

The limitations are that the population studied is within a Canadian context and that the sample was obtained through an Internet panel survey. The study is therefore subject to the biases that this context might entail. The large sample size and the structured sample, however, go some way to ensuring that the sample was representative. The biggest limitation is that the study was designed and conducted for other purposes and lacked some of the data, particularly beliefs and attitudes, that could have supported a more complete model. Further research is needed to 'flesh out' the model. Specifically, following the Theory of Reasoned Action (Fishbein and Ajzen1980), intentions need to be incorporated as well as self efficacy. A redefinition of attitude concepts is also in order.

Consumers are both victims and a key part of the defence against identity theft and fraud. A better understanding of the factors that influence their defensive behaviours is key to controlling "the greatest threat to consumers today" (Snow, 2003).

REFERENCES

Barker, Katherine J., D'Amato, Jackie & Sheridon, Paul (2008). Credit card fraud: awareness and prevention. *Journal of Financial Crime.* Vol.15, 4, 398-410.

BMO (2006), "Reduce Your Roaming Risks: A Portable Privacy Primer", http://www.ipc.on.ca/images/Resources/up-bmo_ipc_priv.pdf accessed 30 June, 2010

Institute for Prospective Technological Studies (2005). Biometrics at the Frontier: Assessing the Impact on Society, Joint Research Centre, European Commission, ftp://ftp.jrc.es/pub/EURdoc/eur21585en.pdf accessed 12 August, 2010

Cavoukian, Ann (2005) Identity Theft Revisited: Security is Not Enough, http://www.ipc.on.ca/images/Resources/idtheft-revisit.pdf accessed 30 June, 2010

Chatterjee, Samprit & Hadi, Ali S. (1986). Influential Observations, High Leverage Points, and Outliers in Linear Regression, *Statistical Science*, Vol. 1, No. 3 (Aug.), pp. 379-393

Comrey, A. I., & Lee, H. B. (1992). *A first course in factor analysis* (2nd ed.) Hillsdale, NJ: Erlbaum.

Consumer Measures Committee (2007). Consumer Identity Theft Kit, http://www.ic.gc.ca/eic/site/cmc-cmc.nsf/vwapj/Consumer%20Kit.pdf/$FILE/Consumer%20Kit.pdf accessed 12 August, 2010

Eisenstein, E. M. (2008). Identity theft: An exploratory study with implications for marketers. *Journal of Business Research*, 11, 1160-1172.

Federal Trade Commission (2003). Identity Theft Survey Report. http://www.ftc.gov/bcp/edu/microsites/idtheft/downloads/synovate_report.pdf accessed 21 Feb, 2011.

Federal Trade Commission (2006) Take Charge: Fighting Back Against Identity Theft, http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf accessed 17 Feb, 2010

Federal Trade Commission (no date) Fighting Back Against Identity Theft, http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html 21 Feb, 2011

Fishbein, Martin and Ajzen, Icek (1980). Understanding attitudes and predicting social behavior, Englewood Cliffs, N.J.: Prentice-Hall.

Jamieson, R., Winchester, D. & Smith, S. (2007). Development of a conceptual framework for managing identity fraud., *Proceedings of the 40th Hawaii International Conference on System Sciences.*

Javelin Strategy and Research (2006). Identity fraud survey report, in Javelin strategy and research, Ed. Hacienda, CA.

Kahn, C. M. & Roberds, W. (2008). Credit and identity theft, *Journal of Monetary Economics*, 2, pp. 251, March.

Kaiser, H. F. (1970). A second-generation Little Jiffy. *Psychometrika*, Vol. 35, pp. 401-415.

Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika*, Vol. 39, pp. 31-36.

Kim, C.; Storer, B. E. (1996) Reference values for Cook's distance, *Communications in statistics. Simulation and computation*, Vol. 25, no 3, pp. 691-708.

Lorenz, Frederick O. (1987) Teaching about Influence in Simple Regression, *Teaching Sociology*, Vol. 15, No. 2 pp. 173-177.

Meyers, L. S., Gamst, G., & Guarino, A. J. (2006) *Applied Multivariate Research: Design and Interpretation.* Thousand Oaks, CA: Sage Publications.

Milne, George R., Labrecque, Lauren I. & Cromer, Cory (2009). Toward an understanding of the online consumer's risky behavior and protection practices. *Journal of Consumer Affairs*, 3,449-473.

Milne, George R., Rohm, Andrew J. & Bahl, Shalini (2004). Consumers' Protection of Online Privacy and Identity. *Journal of Consumer Affairs*, 2, 217-232.

Norberg, Patricia A., Horne, Daniel R. & Horne, David A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors, Journal *of Consumer Affairs*, 1, 100 126.

Rifon, Nora J., LaRose, Robert & Choi, Sejung Marina (2005). Your Privacy Is Sealed: Effects of Web Privacy Seals on Trust and Personal Disclosures. *Journal of Consumer Affairs*, 2, 339 362.

Snow, John (2003). *United States Treasury Secretary John W. Snow: remarks advocating the renewal of the Fair Credit Reporting Act*. Washington, DC: The Treasury Department; June 30. http://www.treasury.gov/press-center/press-releases/Pages/js515.aspx accessed 21 Feb, 2011.

Sproule, S. and Archer, N. (2007). Defining identity theft, *2007 World Congress of the Management of e-Business* (pp.163-173). Los Alamitos, CA163-173.

Sproule, Susan and Archer, Norm (2008). Measuring Identity Theft in Canada 2006 Consumer Survey, McMaster eBusiness Research Centre (MeRC), Working Paper #21, January http://www.merc-mcmaster.ca/working-papers/21.html accessed 17 Feb, 2010

Sproule, Susan and Archer, Norm (2008b). Measuring Identity Theft in Canada 2008 Consumer Survey, McMaster eBusiness Research Centre (MeRC), Working Paper #23, July http://www.merc-mcmaster.ca/working-papers/23.html accessed 17 Feb, 2010

Williams, Dave Arthur (2007). Credit card fraud in Trinidad and Tobago. *Journal of Financial Crime.*Vol.14, 3, 340-359.

Appendix A

2008 Consumer IDT/F Questionnaire - Excerpts

Screening and Quotas

2. How many bank accounts (chequing or savings) do you have?

0 (participant to be screened out)
1
2
3
4
5
More than 5
Prefer not to answer

3. How many credit cards do you have?

0 (participant to be screened out)
1
2
3
4
5
More than 5
Prefer not to answer

4. What is your age?

Under 18 (participant to be screened out)
18-24
25-34
35-44
45-54
55-64
65 or over

5. Are you?

Male
Female

6. Where do you live?

Newfoundland and Labrador
Prince Edward Island
Nova Scotia
New Brunswick
Ontario
Quebec
Manitoba
Saskatchewan
Alberta
British Columbia
Other

Credit Card Fraud

7. *Credit card fraud* occurs when someone makes purchases or otherwise puts charges on a credit card account without your permission. Credit cards include bank-issued credit cards such as Visa, MasterCard, and American Express, as well as retail store-brand credit cards, such as The Bay, Sears, Canadian Tire and others.

Examples of *credit card fraud* include:

- Someone steals your wallet and uses your credit card to make purchases at a store
- The credit card company phones to verify a purchase that you have not made or authorized.
- You notice unauthorized purchases on your monthly statement.

Has *credit card fraud* ever happened to you?

Yes **(Go to 8.)**
No **(Go to 12.)**
8. Has *credit card fraud* happened to you in the last year?

Yes **(Go to 9.)**
No **(Go to 12.)**

Existing Account Fraud

12. *Existing account fraud* occurs when someone gains access to one of your existing accounts (other than a credit card account) without your permission and runs up charges or takes money from the account. This could be a bank account, a telephone account, a utility account, a line-of-credit or loan, or an online account such as an eBay or PayPal account.

Examples of *existing account fraud* are:

- Someone takes your cheque book and forges your name on a number of cheques
- Someone obtains your debit/bank card information, including your PIN, and money is withdrawn from your bank account.
- You receive your phone bill and there are a number of expensive long distance calls that you did not make. The phone company representative tells you that someone used your calling card number and your PIN to make the calls.
- You move, but the new resident continues to have telephone and electric utility services billed to your account.
- Your roommate uses your computer to list fraudulent items for auction under your name and your eBay account.

Has *existing account fraud* ever happened to you?

Yes **(Go to 13.)**
No **(Go to 16.)**

13. Has *existing account fraud* happened to you in the last year?

Yes **(Go to 14.)**
No **(Go to 16.)**

New Account Fraud
16. *New account fraud* occurs when someone uses your personal information to obtain new credit cards, loans, or other accounts, such as telephone accounts or utility accounts, and runs up debts in your name.

Examples of *new account fraud* are:

- Someone opens up a new credit card account in your name and charges purchases on the card which you are then expected to pay for.
- Someone takes out a loan, opens a line of credit or takes out a mortgage on your house in your name
- Someone gives your personal information to open a new cellular telephone account and runs up a phone bill in your name.

Has *new account fraud* ever happened to you?

Yes **(Go to 17.)**
No **(Go to 19.)**

17. Has *new account fraud* happened to you in the last year?

Yes **(Go to 18.)**
No **(Go to 19.)**

Other Identity Fraud

19. *Other identity frauds* occur when someone uses your personal information to impersonate you to gain employment, receive benefits, avoid criminal prosecution or otherwise commit fraud or other crimes.

Examples of *other identity frauds* are:

- You receive a notice from the Canada Revenue Agency that you owe income tax from a job that you never had.
- A friend or neighbour gives your name and address as his or her own when he or she is arrested.
- Someone applies for car insurance using your personal information
- You find out that someone who worked in your home used your personal information to get a replacement health card and obtain health care services under your name.

Has *other identity fraud* ever happened to you?

Yes **(Go to 20.)**
No **(Go to 22.)**

20. Has *other identity fraud* happened to you in the last year?

Yes **(go to 21.)**
No **(go to 22.)**

Data breaches

Note: Question 36 is asked if the respondent has never been a victim of any kind of identity fraud. We do not ask this question of people who have ever been victims.

36. Even if you have not been a victim of any of the above frauds, are you aware of any situations in which your personal information has been accessed or obtained by unauthorized people?

Examples of this could include:

- You receive a notice from your insurance company that a computer or a disc with client information has been lost or stolen.

- You hear that a fellow employee has been charged with fraud for accessing other employees' personal information and selling it to a fraud ring.
- You receive a notice from a company informing all of their clients that someone has hacked into their database and stolen clients' personal information.

Have any of these situations ever happened to you?

Yes **(Go to 37.)**
No **(Go to 42.)**

37. Have any of these situations, where your personal information was accessed or obtained by unauthorized people, happened to you in the last year?

Yes **(Go to 38.)**
No **(Go to 42.)**

Concern
42. How concerned are you about becoming a victim of identity theft in the future? (Check one)

Not at all concerned
Slightly concerned
Somewhat concerned
Very concerned
Extremely concerned
Don't know / Not sure

43. Would you say that your level of concern about becoming a victim of identity theft is higher, lower or about the same as it was one year ago? (Check one)

Higher
About the same
Lower
Don't know / Not sure

Phishing
44. In the last year, have you received emails from a bank or other company asking you to verify or update your account information? (Check one)

Yes **(Go to 45.)**
No **(Go to 46.)**

Behaviour

46. For each of the following activities, please check the most appropriate answer.

MATRIX COLUMNS

All of the time
Most of the time
Some of the time
Rarely
Never
Not applicable

MATRIX ROWS

I use a locked mailbox for incoming mail

I shred financial or important documents before discarding them

I keep sensitive financial information in a secure location, such as a locked drawer or box.

I make sure no one is watching when using an automated banking machine (ABM) or debit machine at a checkout counter.

I use anti-virus, anti-spyware and firewall software that is up-to-date on my computer

I select "remember my card number" or "remember my password" for online log-ins. (REVERSE)

I have different passwords for different applications or services

I use hard-to-break passwords. (i.e. avoid using family member's names or common dictionary words and include special characters and numbers in passwords.)

I give personal information over the phone to people who claim to do surveys, or people offering products or services at special prices. (REVERSE)

I educate children not to disclose personal information in Internet chat rooms or even to family friends without parents' approval.

I respond to a business by clicking on a link in an email. (REVERSE)

I know the approximate balance of my account to compare to the balance shown when withdrawing cash at an Automated Banking Machine (ABM).

47. How often do you do the following?

MATRIX COLUMNS

Daily
Every few days
Every few weeks
Every few months
Yearly
Every 2-5 years
Every 5 or more years
Never
Not applicable

MATRIX ROWS

Monitor bank account balances and activity
Monitor credit card accounts and activity
Request a copy of your credit report
Check Land Registry Office records to ensure validity of ownership
Change important passwords (i.e. for online banking, email accounts, etc.)

48. Because of a concern about identity theft, have you done any of the following?

MATRIX COLUMNS

In the last year
In the last 2-5 years
More than 5 years ago
Never

MATRIX ROWS

Subscribed to a credit monitoring service
Paid for identity theft insurance
Asked for a credit alert to be placed on your credit report

Additional Demographics

50. What is your highest level of education?

Some/completed elementary school
Some/completed high school
Some/completed technical school

Some/completed community college/ CEGEP
Some/completed university
Some/completed graduate school
Prefer not to answer

51. What is your marital status?

Single, never married
Married or living together
Separated or divorced
Widowed
Prefer not to answer

52. Including yourself, how many people are there in your household who are…

Adults 18 years and older
Teens 13 to 17 years of age
Children 7 to 12 years of age
Children 6 and under
Prefer not to answer

(answers must be a positive whole number, except prefer not to answer which is a regular checkbox)

53. What is your total household income?

Less than $25,000
$25,000-49,999
$50,000-74,999
$75,000-99,999
$100,000 or more
Prefer not to answer

Appendix B – Demographic Statistics

Age

	Frequency	Percent
18-24	319	10.6
25-34	689	22.8
35-44	705	23.4
45-54	511	16.9
55-64	559	18.5
> 64	233	7.7
Total	3016	100.0

Gender

	Frequency	Percent
Male	1408	46.7
Female	1608	53.3
Total	3016	100.0

Province

	Frequency	Percent
Newfoundland	68	2.3
British Columbia	383	12.7
PEI	17	.6
Nova Scotia	115	3.8
New Brunswick	81	2.7
Ontario	1075	35.6
Quebec	814	27.0
Manitoba	108	3.6
Saskatchewan	101	3.3
Alberta	254	8.4
Total	3016	100.0

Education

	Frequency	Percent
Elementary	12	.4
High	531	17.6
Technical	304	10.1
College	820	27.2
University	1009	33.5
Graduate School	305	10.1
Prefer Not to Answer	35	1.2
Total	3016	100.0

Marital Status

	Frequency	Percent
Single	777	25.8
Married	1818	60.3
Separated	312	10.3
Widowed	63	2.1
Prefer Not to Answer	46	1.5
Total	3016	100.0

Household Income

	Frequency	Percent
< $25,000	247	8.2
$25,000 - $49,999	673	22.3
$50,000 - $74,999	623	20.7
$75,000 - $99,999	381	12.6
$100,000 or More	390	12.9
Prefer Not to Answer	702	23.3
Total	3016	100.0

Appendix C – Descriptive Statistics

		Std.		
	Mean	Deviation	Skewness	Kurtosis
2 Number of Bank Accounts	2.3095	1.17294	1.158	1.361
3 Number of Credit Cards	2.5318	1.49813	.933	-.042
4 Age	45.7043	15.93051	.066	-1.139
42 Concern Level	3.2160	1.03429	-.004	-.494
43 Concern Change	1.6672	.49594	-.414	-1.118
46.1 Use Locked Mailbox	3.4284	1.84356	-.449	-1.693
46.2 Shred Documents	4.1814	1.21674	-1.454	.990
46.3 Locked Financial Information	3.4733	1.51006	-.472	-1.273
46.4 No One Watches at ATM	4.4301	.81848	-1.545	2.268
46.5 Use Antivirus Software	4.6945	.70796	-2.875	9.247
46.6 Use Remember Password	3.6661	1.44116	-.629	-1.010
46.7 Use Different Passwords	3.6695	1.18847	-.576	-.563
46.8 Use Hard-to-break Passwords	4.1027	1.05676	-1.058	.335
46.9 Give Personal Info Over Phone	4.6074	.72785	-2.256	5.990
46.10 Educate Children	4.1426	1.20366	-1.353	.793
46.11 Click on e-mail Link	3.9489	1.00915	-.702	-.093
46.12 Approximate Balance Compare at ATM	4.4764	.72851	-1.563	2.901
47.1 Monitor Bank Balance	6.9453	.79760	-1.623	8.976
47.2 Monitor Credit Card	6.5202	.94296	-1.549	7.582
47.3 Get Credit Report	2.6889	1.99412	.836	-.430
47.4 Check Land Registry	1.6457	1.44236	2.558	6.417
47.5 Change Passwords	3.3982	1.94769	.203	-.950
50 Household Income	2.9661	1.26489	.216	-1.002
50 Imputed Household Income	2.93	1.252	.202	-.935

Weighted to reflect the structured sample. See Appendix F.

Appendix D – Not Applicable/Declined/Don't Know Responses

Question #	***Question***	# N/A*	% N/A
42	Concern Level	19.31	0.64
43	Concern Change	26.56	0.88
46.1	Use locked mailbox	220.11	7.30
46.2	Shred documents	27.58	0.91
46.3	Locked financial information	49.95	1.66
46.4	No one watches at ATM	44.70	1.48
46.5	Use antivirus software	18.22	0.60
46.6	Use remember passwords	52.32	1.73
46.7	Use different passwords	44.92	1.49
46.8	Use hard-to-break passwords	17.58	0.58
46.9	Give personal information over the phone	49.64	1.65
46.10	Educate children	1,199.22	39.76
46.11	Click on e-mail link	159.14	5.28
46.12	Approximate balance comparison at ATM	63.24	2.10
47.1	Monitor bank balance	8.39	0.28
47.2	Monitor credit card	11.19	0.37
47.3	Get credit report	95.46	3.17
47.4	Check land registry	746.45	24.75
47.5	Change passwords	117.44	3.89
50	Household Income	723.76	24.00

* Weighted to reflect the structured sample. See Appendix F.

Appendix E - Correlations

	46.1	46.2	46.3	46.4	46.5	46.6	46.7	46.8	46.9	46.10	46.11	46.12	47.1	47.2	47.3	47.4	47.5
46.1 Use Locked Mailbox	1.000																
46.2 Shred Documents	.136**	1.000															
46.3 Locked Financial Information	.202**	.390**	1.000														
46.4 No One Watches at ATM	.117**	.332**	.402**	1.000													
46.5 Use Antivirus Software	.118**	.172**	.212**	.280**	1.000												
46.6 Use Remember Password	.006	.063**	.022	.083**	.034*	1.000											
46.7 Use Different Passwords	.053**	.170**	.234	.231**	.142**	.045**	1.000										
46.8 Use Hard-to-break Passwords	.090**	.208**	.256**	.296**	.187**	.055**	.367**	1.000									
46.9 Give Personal Info Over Phone	.043**	.092**	.090**	.107**	.054**	.144**	.069**	.128**	1.000								
46.10 Educate Children	.043**	.187**	.223**	.288**	.180**	.066**	.123**	.188**	.075**	1.000							
46.11 Click on e-mail Link	-.025	.045**	.025	.053**	.071**	.138**	.052**	.059**	.200**	.054**	1.000						
46.12 Approximate Balance Compare at ATM	.060**	.209**	.225**	.310**	.257**	.022	.213**	.249**	.082**	.235**	.080**	1.000					
47.1 Monitor Bank Balance	.055**	.067**	.099**	.096**	.110**	-.008	.107**	.089**	.033*	.087**	.038*	.315**	1.000				

47.2 Monitor Credit Card	.052**	.068**	.157**	.138**	.096**	.023	.133**	.133**	.040*	.078**	.030*	.252**	.608**	1.000			
47.3 Get Credit Report	.071**	.051**	.210**	.105**	.026	-.047**	.126**	.103**	-.010	.059**	-.035*	.078**	.155**	.228**	1.000		
47.4 Check Land Registry	.049**	.045**	.165**	.091**	.028	-.062**	.118**	.102**	-.026	.062**	-.084**	.054**	.117**	.199**	.432**	1.000	
47.5 Change Passwords	.037*	.123**	.195**	.178**	.103**	.053**	.344**	.220**	.027	.100**	-.035*	.122**	.154**	.206**	.257**	.305**	1.000

**. Correlation is significant at the 0.01 level (1-tailed).

*. Correlation is significant at the 0.05 level (1-tailed).

Appendix F – Weights

		Gender					
		Male			Female		
		Population	Sample	Weight	Population	Sample	Weight
Province	**Age**						
Newfoundland	**18-24**	24,903	0	0.000	24,668	4	0.740
	25-34	30,287	4	0.909	31,989	7	0.548
	35-44	40,996	13	0.378	42,460	15	0.340
	45-54	41,156	6	0.823	42,398	6	0.848
	55-64	33,784	5	0.811	34,117	4	1.024
	>64	30,314	4	0.909	37,431	0	0.000
PEI	**18-24**	7,025	0	0.000	6,992	2	0.420
	25-34	7,817	1	0.938	8,273	1	0.993
	35-44	10,091	2	0.605	10,485	2	0.629
	45-54	9,972	6	0.199	10,512	2	0.631
	55-64	8,357	0	0.000	8,609	0	0.000
	>64	8,423	1	1.011	11,028	0	0.000
Nova Scotia	**18-24**	45,605	1	5.473	43,679	4	1.310
	25-34	56,030	7	0.961	58,610	22	0.320
	35-44	74,245	19	0.469	74,718	19	0.472
	45-54	71,201	4	2.136	73,948	9	0.986
	55-64	57,971	15	0.464	58,821	6	1.176
	>64	57,529	8	0.863	76,042	1	9.125
New Brunswick	**18-24**	36,778	3	1.471	34,268	5	0.822
	25-34	47,470	6	0.949	47,767	11	0.521
	35-44	59,984	15	0.480	59,181	7	1.015
	45-54	58,170	6	1.163	59,788	8	0.897
	55-64	46,625	7	0.799	46,480	6	0.930
	>64	44,857	5	1.077	59,854	2	3.591
Ontario	**18-24**	610,467	31	2.363	587,286	55	1.281
	25-34	839,990	85	1.186	848,188	156	0.652
	35-44	1,060,346	86	1.480	1,047,059	135	0.931
	45-54	902,452	88	1.231	926,444	123	0.904
	55-64	656,773	107	0.737	676,054	121	0.670
	>64	702,037	52	1.620	906,661	36	3.022
Quebec	**18-24**	350,417	52	0.809	334,214	94	0.427
	25-34	519,077	107	0.582	499,401	93	0.644
	35-44	606,776	85	0.857	582,740	125	0.559
	45-54	592,352	68	1.045	604,381	33	2.198
	55-64	454,643	91	0.600	470,403	27	2.091
	>64	439,012	32	1.646	606,649	7	10.40

		Gender					
		Male			Female		
		Population	Sample	Weight	Population	Sample	Weight
Manitoba	**18-24**	60,488	5	1.452	57,241	3	2.290
	25-34	77,841	9	1.038	74,863	17	0.528
	35-44	89,200	10	1.070	85,997	15	0.688
	45-54	84,119	11	0.918	83,810	9	1.117
	55-64	60,927	12	0.609	61,881	11	0.675
	>64	67,729	4	2.032	90,860	2	5.452
Saskatchewan	**18-24**	55,002	4	1.650	51,056	5	1.225
	25-34	61,146	13	0.564	59,977	18	0.400
	35-44	68,479	7	1.174	68,346	14	0.586
	45-54	71,706	8	1.076	70,846	11	0.773
	55-64	49,915	7	0.856	49,601	8	0.744
	>64	63,962	4	1.919	83,140	2	4.988
Alberta	**18-24**	179,140	12	1.791	168,239	16	1.262
	25-34	253,015	25	1.214	235,644	29	0.975
	35-44	266,552	20	1.599	254,168	32	0.953
	45-54	247,569	17	1.748	240,652	25	1.155
	55-64	155,199	27	0.690	152,645	24	0.763
	>64	152,098	17	1.074	188,455	10	2.261
British Columbia	**18-24**	213,967	8	3.210	203,362	15	1.627
	25-34	274,596	27	1.220	275,712	51	0.649
	35-44	342,523	33	1.246	346,036	51	0.814
	45-54	321,979	33	1.171	331,673	38	1.047
	55-64	248,109	44	0.677	248,910	37	0.807
	>64	265,531	29	1.099	321,225	17	2.267

Appendix G – Principal Components Analysis of Data with Listwise Deletion of 'Not Applicable'.

Pattern Matrix

	Factor1	Factor2	Factor3	Factor4	Factor5
47.1 Monitor Bank Balance	**0.91907**	-0.06385	-0.00745	0.01049	-0.01620
47.2 Monitor Credit Card	**0.86527**	0.07997	0.02346	0.00269	0.01906
47.3 Get Credit Report	0.02521	**0.86037**	-0.02487	0.00110	0.03986
47.4 Check Land Registry	-0.00557	**0.85383**	0.02103	-0.01583	-0.04468
46.7 Use Different Passwords	0.03082	0.02967	**0.81135**	-0.04629	-0.03459
46.8 Use Hard-to-break Passwords	0.01449	-0.00493	**0.75926**	0.07627	0.03528
46.1 Use Locked Mailbox	0.03824	0.00412	-0.25507	**0.76112**	-0.03065
46.2 Shred Documents	-0.00629	-0.10317	0.24359	**0.64603**	0.04456
46.3 Locked Financial Information	0.00417	0.18162	0.25293	**0.61792**	0.02374
46.9 Give Personal Info Over Phone	-0.02584	0.05212	0.01681	0.07841	**0.68687**
46.11 Click on e-mail Link	0.04857	-0.03954	0.04637	-0.12905	**0.68392**
46.6 Use Remember Password	-0.01551	-0.01472	-0.06897	0.03525	**0.62339**

Structure Matrix

	Factor1	Factor2	Factor3	Factor4	Factor5
47.1 Monitor Bank Balance	**0.88857**	-0.06095	-0.00716	0.01022	-0.01594
47.2 Monitor Credit Card	**0.83655**	0.07633	0.02258	0.00262	0.01876
47.3 Get Credit Report	0.02437	**0.82122**	-0.02394	0.00107	0.03923
47.4 Check Land Registry	-0.00538	**0.81498**	0.02024	-0.01542	-0.04397
46.7 Use Different Passwords	0.02980	0.02832	**0.78075**	-0.04509	-0.03405
46.8 Use Hard-to-break Passwords	0.01401	-0.00470	**0.73063**	0.07430	0.03473
46.1 Use Locked Mailbox	0.03697	0.00393	-0.24545	**0.74144**	-0.03016
46.2 Shred Documents	-0.00608	-0.09847	0.23441	**0.62933**	0.04386
46.3 Locked Financial Information	0.00403	0.17336	0.24339	**0.60194**	0.02337
46.9 Give Personal Info Over Phone	-0.02498	0.04975	0.01617	0.07639	**0.67605**
46.11 Click on e-mail Link	0.04696	-0.03774	0.04462	-0.12571	**0.67314**
46.6 Use Remember Password	-0.01499	-0.01405	-0.06637	0.03434	**0.61357**

Appendix H – Principal Components Analysis of Data with Listwise Deletion of 'Not Applicable' and deletion of 106 'outlying' cases.

Pattern Matrix

47.1 Monitor Bank Balance	**0.91761**	-0.04784	-0.01885	0.01967	-0.02515
47.2 Monitor Credit Card	**0.85837**	0.09662	0.03683	0.00768	0.03532
47.3 Get Credit Report	0.01906	**0.86389**	-0.01653	-0.00955	0.04210
47.4 Check Land Registry	0.01354	**0.85412**	0.01563	-0.01198	-0.04485
46.7 Use Different Passwords	0.03780	0.03065	**0.81168**	-0.05351	-0.03810
46.8 Use Hard-to-break Passwords	0.00298	-0.00198	**0.75181**	0.07867	0.05176
46.1 Use Locked Mailbox	0.05320	0.00551	-0.27300	**0.76992**	-0.02312
46.2 Shred Documents	-0.03112	-0.08788	0.24910	**0.64307**	0.03644
46.3 Locked Financial Information	0.01971	0.16145	0.27888	**0.60068**	0.02008
46.11 Click on e-mail Link	0.12884	-0.09156	0.02245	-0.09764	**0.66854**
46.9 Give Personal Info Over Phone	0.02886	0.04207	0.03998	0.06858	**0.66359**
46.6 Use Remember Password	-0.12652	0.03384	-0.06099	0.01942	**0.65453**

Structure Matrix

47.1 Monitor Bank Balance	**0.89083**	-0.04584	-0.01811	0.01911	-0.02479
47.2 Monitor Credit Card	**0.83331**	0.09259	0.03538	0.00746	0.03481
47.3 Get Credit Report	0.01850	**0.82782**	-0.01588	-0.00927	0.04150
47.4 Check Land Registry	0.01314	**0.81846**	0.01501	-0.01164	-0.04420
46.7 Use Different Passwords	0.03669	0.02937	**0.77989**	-0.05199	-0.03755
46.8 Use Hard-to-break Passwords	0.00289	-0.00190	**0.72236**	0.07643	0.05102
46.1 Use Locked Mailbox	0.05164	0.00528	-0.26231	**0.74800**	-0.02279
46.2 Shred Documents	-0.03021	-0.08421	0.23934	**0.62476**	0.03592
46.3 Locked Financial Information	0.01913	0.15471	0.26796	**0.58357**	0.01979
46.11 Click on e-mail Link	0.12508	-0.08774	0.02157	-0.09486	**0.65893**
46.9 Give Personal Info Over Phone	0.02802	0.04032	0.03841	0.06662	**0.65405**
46.6 Use Remember Password	-0.12283	0.03243	-0.05860	0.01887	**0.64513**

McMaster University
1280 Main St. W. DSB A202
Hamilton, ON
L8S 4M4

Tel: 905-525-9140 ext. 23956
Fax: 905-528-0556
Email: ebusiness@mcmaster.ca
Web: http://merc.mcmaster.ca