CONSUMER IDENTITY THEFT PREVENTION AND DETECTION BEHAVIOURS

CONSUMER IDENTITY THEFT PREVENTION AND IDENTITY FRAUD DETECTION BEHAVIOURS: AN APPLICATION OF THE THEORIES OF PLANNED BEHAVIOUR AND PROTECTION MOTIVATION

by JOHN A. GILBERT, B.Sc., M.B.A.

A Thesis Submitted to the School of Graduate Studies

In Partial Fulfilment of the Requirements for the Degree of

Doctor of Philosophy

McMaster University

McMaster University DOCTOR OF PHILOSOPHY (2014) Hamilton, Ontario (Business)

TITLE: Consumer Identity Theft Prevention and Identity Fraud Detection Behaviours:
An Application Of The Theories Of Planned Behaviour And Protection Motivation

AUTHOR: John A. Gilbert, B.Sc. (McMaster University), M.B.A. (McMaster University)

SUPERVISOR: Professor Norman P. Archer

PAGES: xi, 280

ABSTRACT

Consumer behaviour has and may increasingly have a vital role to play in protecting personal data. Understanding the behaviours of consumers in preventing identity theft and detecting identity fraud is therefore key to creating programs that minimize exposure and potential loss. In this study, based on the Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT), an exploratory study elicited salient beliefs about identity theft prevention and detection behaviours. These beliefs were then used to create a survey to measure the strength of the salient beliefs, attitudes, intentions and behaviours, which was administered online and produced 351 valid responses. Statistical analysis was performed on eight behavioural groups, based primarily on principal component analysis of twelve behaviours. The groups were: using physical security, practicing password security, monitoring bank accounts and credit cards, getting a credit report, checking the land registry, using 'remember my password', clicking on a link in an e-mail, and giving out personal information over the phone. Results showed that beliefs with a significant influence on consumer intentions for a given behavioural group were a mix of beliefs about identity theft in general and beliefs about the behaviours in that group. While attitudes towards behaviours of consumers in any specific group had a significant influence on the intent to perform behaviours peculiar to that group, they had virtually no impact on the intent to perform behaviours in other groups. The intent to perform identity theft prevention and identity fraud detection behaviours uniformly had a statistically significant influence on actual reported behaviour, but much of the variance in behaviour was unexplained. An analysis of qualitative responses showed that gender, language and age all had significant impacts on respondents' likelihood of mentioning specific vulnerabilities, and prevention and detection measures.

ACKNOWLEDGMENTS

There are many people whose help and support were essential in the completion of this journey. This brief note goes but a little way to acknowledge their contribution.

First of all, I would like to thank the DeGroote community. My colleges in the business school have always been willing to discuss problems, issues and approaches and I appreciate their openness and thank them for their support. I would particularly like to thank John Laugesen who took time from work on his own dissertation to be an additional coder on the Phase 1 exploratory study. I would also like to thank the faculty and staff of the DeGroote Business School for their help and support along the way and in particular Carolyn Colwell, Deb Randall-Baldry, Iris Kehler, Sandra Stephens, Dr. Yufei Yuan, Dr. Aaron Schat, Dr. Catherine Connelly, Dr. Vishwanath Baba and Dr. Milena Head. I would also like to thank the business school for the research grant that made this investigation financially possible.

I would like to thank the members of my supervisory committee, Dr. Brian Detlor and Dr. Nick Bontis for their helpful suggestions and guidance.

To my supervisor, Dr. Norm Archer many thanks. The wisdom and patience that only comes from years of experience is greatly appreciated. I cannot count the number of times I was grateful to have you as my supervisor. You are a gem.

Finally I would like to thank my family for their support both moral and practical. I thank my children, Erika and Geoffrey not only for their patience when I was physically and/or mentally occupied, but also for their help in being 'guinea pigs' on early versions of the surveys. I would also like to thank Erika, who started grad school the same time I did, for being the additional

coder for the qualitative portion of the Phase 2 survey. Last, but not least, to my wife, Constance (Dina), who admits to being a compulsive editor, many thanks for the reviews of the many revisions of the dissertation and the surveys. You are my favourite person in the world and your support has been essential in getting this far.

Table of Contents

List of Tables

List of Figures

List of Abbreviations and Definitions

APC	Average Path Coefficient (measure of PLS model fit)
APCA	Australian Payments Clearing Association
ARS	Average R Squared (measure of PLS model fit)
AVE	Average Variance Extracted
Dumpster diving	Retrieving personal information from the trash
Existing account fraud	A financial identity fraud where the criminal uses an existing account such as a credit card or bank account by pretending to be the real owner
Financial identity fraud	An identity fraud involving a financial instrument such as a credit card, mortgage or other loan
FTC	Federal Trade Commission (U.S.)
Identity theft	Obtaining personal identity information without just cause (Depending on the legal jurisdiction, this may be a crime in and of itself without the information being used fraudulently.)
Identity fraud	Crime committed using a false identity
ITADA	Identity Theft and Assumption Deterrence Act (U.S.)
ITRC	Identity Theft Resource Center (U.S.)
IRS	Internal Revenue Service (U.S.)
MANOVA	Multivariate Analysis of Variance
New account fraud	A financial identity fraud where the criminal opens a new account, such as a credit card or home equity loan, using a false identity
Non-financial identity fraud	Using a false identity for a crime not directly involving a financial instrument (The most prevalent form is if someone uses a false identity when he or she is arrested for another crime.)
OECD	Organization for Economic Co-operation and Development
Phishing	The fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information online
PLS	Partial Least Squares (an SEM technique)
PIPEDA	Personal Information Protection and Electronic Documents Act (Canada)
PBC	Perceived Behavioural Control (part of TPB)
PMT	Protection Motivation Theory
SEM	Structural Equation Modeling (second generation data analysis techniques)
Synthetic account fraud	A financial identity fraud where the criminal opens a new account, such as a credit card or home equity loan, using an identity created from multiple real people, synthetic information, or a mixture of both
TPB	Theory of Planned Behaviour

Chapter 1. Introduction

The quintessential crimes of the information age are identity theft and the use of stolen identity to commit identity fraud. Occurrences have grown rapidly in recent years due to the widespread use of the Internet by consumers and businesses. Former U.S. Treasury Secretary John Snow called identity theft "the greatest threat to consumers today..." because it "...destroys the trust in both people and financial institutions that is necessary to run an open, modern economy" (Snow, 2003). In addition to the unquantified damage to society that Snow delineated, there are direct consequences to the individuals and businesses affected. The U.S. Federal Trade Commission (FTC) reported that identity theft topped the list of complaints it received in 2012 for the 13th year in a row (FTC, 2013) (see Figure 1). 'Impostor scams', where impostors pose as family, friends or respected organizations, which were in the top 10 list for the first time in 2010

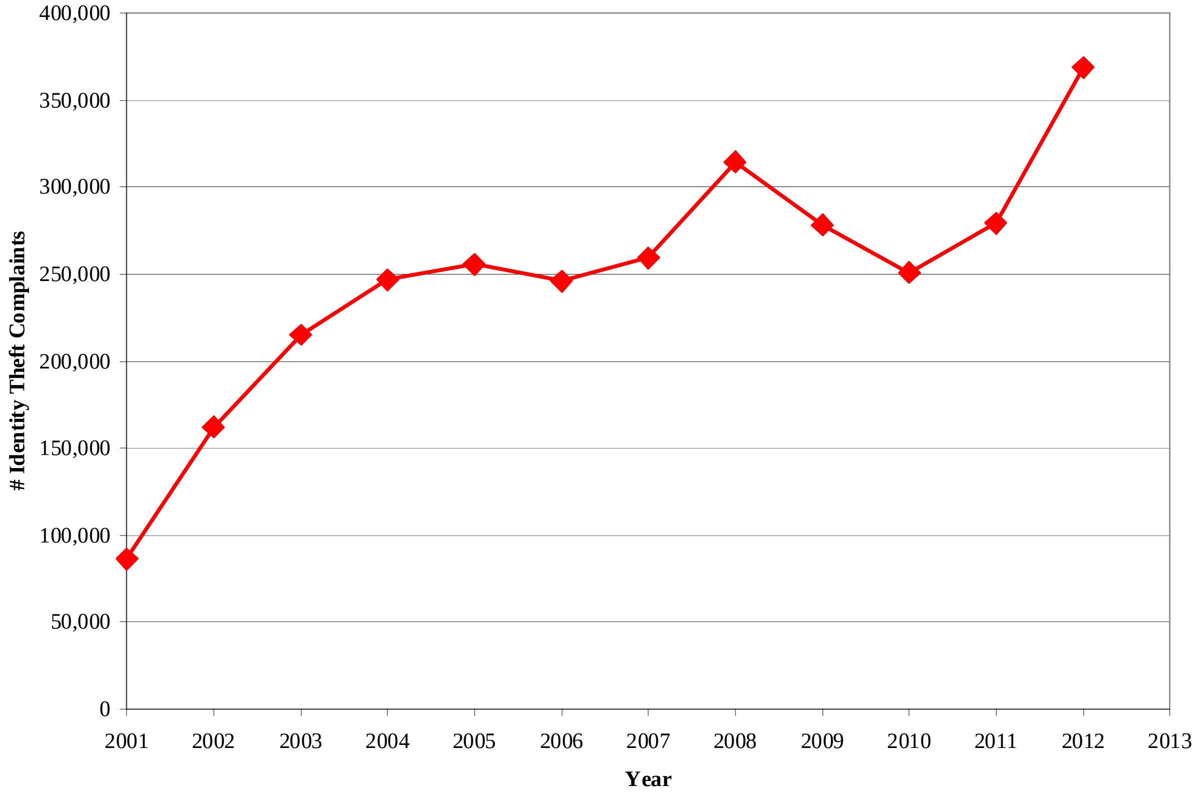


Figure 1 – Number of Identity Theft Complaints in the U.S. (Data from FTC, 2013)

(FTC, 2011), moved up to number 6 in 2012 (FTC, 2013). According to a study by the Bureau of Justice Statistics of the U.S. Department of Justice, 8,571,900 or 7.0% of the households in the U.S. had at least one member who was a victim of one or more types of identity theft in 2010. This was a 33% increase over 2005; the financial loss amounted to $13.2 billion USD (Langton, 2011). In Canada, 6.5% of adults surveyed were victims within a single year, with out-of-pocket costs to the victims amounting to $150 million CAD and 20 million hours to deal with the resulting problems (Sproule and Archer, 2008b). Data from the Australian Payments Clearing Association (APCA, 2013) also show an dramatic increase in credit card fraud since 2006, with the number of fraudulent transactions increasing from 236,271 in 2006 to 1,166,311 in 2012, or a 394% increase. The value of fraudulent transactions increased from $87,432,913 AUD to $262,572,333, or a 200% increase, while the value of all transactions increased by only 81% (see Figure 2 for amounts relative to 2006). In fact, the actual numbers of victims and losses are not accurately known. Crimes are often not reported to police (FTC, 2013) and some individuals may not even know they have been victimized until months after the fact (Newman and McNally, 2005). Given the current rates of identity fraud, *excluding* credit card fraud, on average, every individual will be a victim once during his or her adult life (Anderson et al., 2008).

It seems as if everyone, including business and government, is vulnerable to identity theft and fraud. The Internal Revenue Service (IRS) in the U.S. rejected 260,000 tax returns based on identity theft for the 2011 taxation year, representing $1.3 billion in fraudulent tax refunds (Fisk and Stigile, 2012). The problem for 2011 represented a five-fold increase over the 2008 taxation year. Identity theft and fraud afflicts everyone, including the rich, famous and powerful. Major League Baseball, for example, has had some prominent players who were not who they claimed to be (Kepner, 2012). Even the U.S. Federal Reserve Board chair, Ben Bernanke has been victimized (Isikoff, 2009).

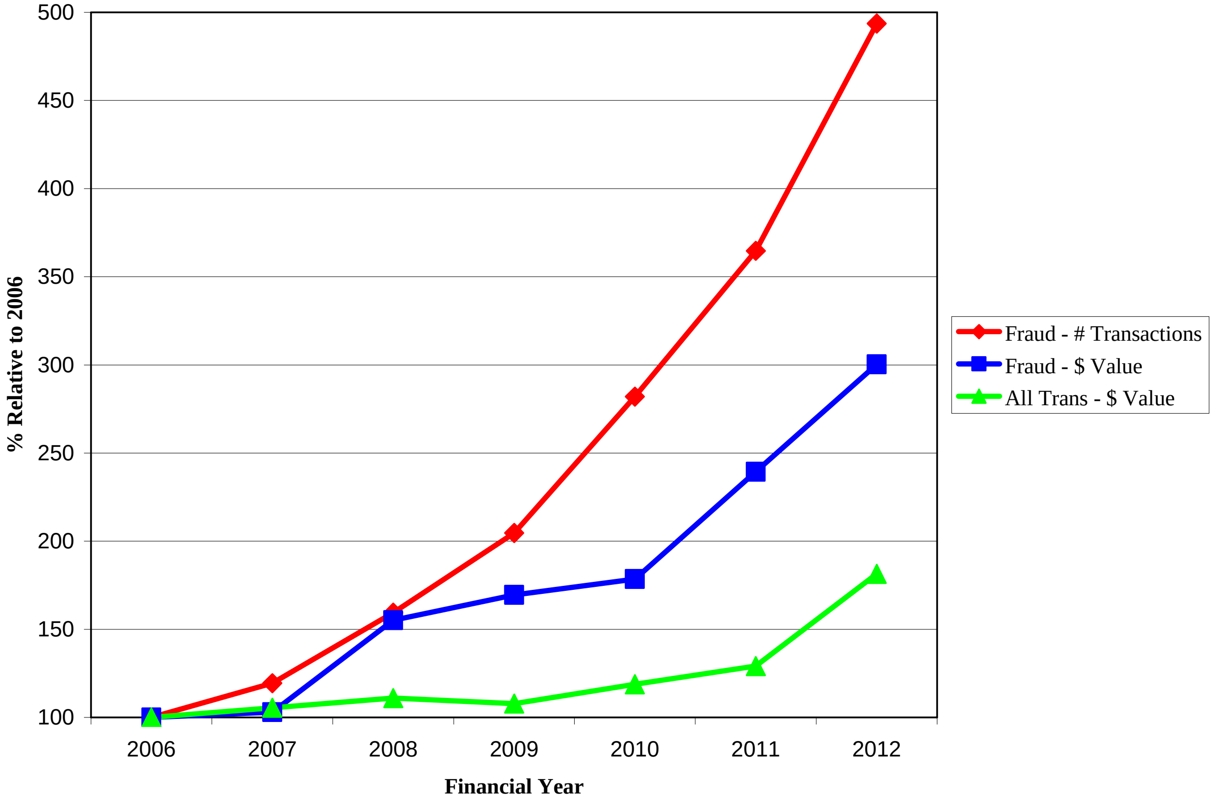


Figure 2 – Credit Card Fraud in Australia Relative to the Year 2006 (Data from APCA, 2013)

Not all of the consequences of identity theft and fraud are financial, however. Many victims report stress due to the time required to correct their records, frustration with agencies, and shock at the realization that someone has been impersonating them (Newman and McNally, 2005). Anderson et al. (2008) report statistics on the non-financial problems suffered by identity fraud victims, which include being harassed by debt collectors, having to repeatedly correct the same information on their credit reports, having credit card problems, being turned down for loans, having banking problems such as rejected cheques, having phone or utility services cut off, being subjects of criminal investigations and to civil suits. In some cases, marriage break-up and loss of livelihood are consequences. Identity thieves in extreme cases committed crimes using the victims' identities, resulting in the arrest of the victims (Newman and McNally, 2007).[1]

[1] For an extreme case of victimization see Kreuter (2003 and 2004). He chronicles the woes of an airline pilot who reported identity theft, was not believed by authorities, labelled as "psychotic" and subsequently stripped of his pilot's licence. And this was only the beginning of the victim's problems.

In addition to the financial and non-financial costs borne by the victims, society at large also bears costs. Fear of identity theft may prevent consumers from making online purchases or seeking credit, which decreases economic activity. Merchants may reject transactions that appear suspicious and spend resources to safeguard their systems and customer information, the costs of which are then passed on to the consumer (Anderson et al., 2008). In a U.S. survey, 15% of respondents indicated that they had reduced or stopped online purchases, 8% reduced or stopped online banking due to concerns about information theft, and 36% only visit sites they are familiar with (National Cyber Security Alliance, 2009). In a later survey, 42% of respondents had stopped or abandoned a purchase on a website during the previous year because of a safety or security concern (National Cyber Security Alliance, 2011). In Canada, 20% of respondents reported reducing or stopping online shopping and 9% reported reducing or stopping online banking over a one-year period (Sproule and Archer, 2008b).

The remarkable growth in identity theft and fraud may be explained by Routine Activity Theory (Cohen and Felson, 1979). The theory holds that crime takes place when likely offenders, suitable targets and the absence of capable guardians against crime converge in space and time. It is the routine activities of both victims and perpetrators that set the stage for crime. For identity theft, societal changes have increased the number of suitable targets and decreased the number of capable guardians. The advent and widespread use of credit and debit cards, the ubiquitous penetration of the Internet, and the wealth of personal information stored in it (particularly in social networking sites) have vastly increased the number of suitable targets for identity theft. In many instances, capable guardianship has not been deployed (Brodkin, 2007, Gilbert and Archer, 2012). Furthermore, asynchronous Internet interactions mean that likely offenders and suitable targets need not converge in space and time, furthering the opportunities for identity theft. All of these factors suggest that, due to changes in routine activities, identity theft has increased and will likely continue to increase. Predictions are that 'millennials', who habitually share more personal information, will continue to do so as they age. The sharing of information will become the norm as the notion of privacy prevailing in the industrial era declines (Anderson and Rainie, 2010).

Responsibility for identity theft prevention (capable guardianship) can be said to fall on three groups: 1) the consumers that own and provide the information, 2) the organizations (including businesses and governments) that collect and use the information, and 3) the legislative bodies (including national and regional governments) that regulate the handling of personal information. Schreft (2007) has shown that, left on its own, the market will not efficiently or effectively control identity theft and fraud. The asymmetric information available to the parties directly involved and the costs external to those parties mean that free-market forces will not optimally manage identity fraud, therefore necessitating a legislative role for governments. The Organization for Economic Co-operation and Development (OECD), for example, emphasizes regulation and calls on its member nations to standardize definitions and statistics, enact legislation to provide legal remedies for the victims and deter the perpetrators, and enforce such legislation (OECD, 2009). Example legislation includes the U.S. Identity Theft and Assumption Deterrence Act (ITADA), the California Privacy Law (SB1386) and the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). European countries tend to not have identity-specific legislation but rather to rely on more traditional provisions such as fraud, forgery and imposture (Koops et al., 2009). There are also philosophical differences between North America and Europe. The EU view is that information privacy is a fundamental right, whereas U.S. legislation is aimed at balancing privacy against efficient commerce. These differences work their way into the definitions of identity crime. U.S. legislation tends to consider identity theft and identity fraud as a single crime, whereas the EU tends to view them separately (Schwartz and Solve, 2013). The perpetrators of Internet identity theft and fraud frequently operate extraterritorially, making it a global issue; international cooperation is therefore essential. Specific agreements include the International Cybercrime Convention (Council of Europe, 2001), which, in addition to being signed by most member states, was also signed by Canada, Japan and the U.S. International agencies involved include the OECD (2009) and Interpol (2010). Deterrents may be ineffectual, however. It is estimated that only 11% of reported identity fraud cases in the U.S. are solved (Newman and McNally, 2007).[2] Often the victim does not even know how the theft occurred (Klein, 2010), and in some cases the identity is a composite of multiple victims' information, none of whom recognize that their information has been misused (Schreft, 2007).

Businesses and governments, as custodians of much collected personal information, also have a role in limiting identity crime. The Identity Theft Resource Center (ITRC) annual report for 2011 lists 419 data breaches in the U.S., exposing 22,918,441 records (Identity Theft Resource Center, 2012). In Canada, the Privacy Commissioner for the province of Ontario lists 15 cases of massive organizational data breaches in the year 2005 (Cavoukian, 2005). In response, governments have enacted legislation requiring organizations to safeguard personal information. In the U.S., several laws and regulations require organizations to protect personal information from illegal access. Examples are the Gramm-Leach-Bliley Act of 1999, which requires financial institutions to protect customer financial information, the Fair and Accurate Credit Transactions Act of 2003, which requires the 'safe' disposition of credit reports, and the Federal Trade Commission Act, which prohibits irresponsible exposure of consumer data. The Red Flag Rule, which came into effect on January 1, 2011, requires all financial institutions and creditors that offer or maintain covered accounts (including credit cards, mortgage or car loans, utility accounts, chequing accounts, and most types of savings accounts) to implement an identity theft prevention program (Kunick and Posner, 2011). There are signs that these legislative initiatives are having some effect. Romanosky, Telag and Acquisti (2011), after controlling for other factors, show a 6% drop in identity fraud in states that have enacted data breach disclosure laws. Retailers are finding, however, that regardless of the legal requirements, customer concerns about information security are limiting business (Murphy, 2008). Concerns about data privacy

[2] Consumer perception of law enforcement is not positive with 65% disagreeing that the local police were equipped to handle reports and investigate crimes over the Internet (National Cyber Security Alliance, 2011).

deter consumers from adopting online services (Lee, 2009, Featherman and Pavlou, 2003). Repeated disclosures of data breaches and associated newspaper headlines have had a significant impact on reputations and can lead to a drop in share price (Acquisti, Friedman and Telang, 2006). In extreme cases, failure to protect identity information has led to bankruptcy and liquidation (Stech, 2012). Identity information security has become a business imperative. As organizations tighten up their information security, however, there are indications that criminals, and in particular organized criminals, are turning to the 'softer' target of the individual consumer (Punch, 2004).

Despite the best efforts of governments and businesses, consumer behaviour still has and may increasingly have a vital role to play in protecting personal data. As Stajano and Wilson (2011) put it, "the weakest point in any security-strengthening system is usually its human element". Kevin Mitnick, one of the world’s most famous hackers, states:

> “The human side of computer security is easily exploited and constantly overlooked. Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain.” (Neumann, 2000)

Businesses and governments have recognized this reality and have encouraged consumer education regarding identity theft prevention and identity fraud detection[3]. Education is not enough, however. Consumers may know what to do but not behave accordingly; for example, less than 10% of consumers affected by the *ChoicePoint* data breach used the free credit monitoring services that were offered (Brodkin, 2007). In Canada, 76.1% of consumers are 'somewhat', 'very' or 'extremely' concerned about the threat of identity theft, but only 33.8% check their credit report at least once a year (Sproule and Archer, 2008b). All but three of the U.S. states have enacted laws allowing customers to ‘freeze’ their credit records, which prevents businesses from accessing them without explicit permission and the three American credit

[3] Examples include Take Charge: Fighting Back Against Identity Theft (FTC 2006), Consumer Identity Theft Kit (Consumer Measures Committee 2007), Identity Theft and You (Office of the Privacy Commissioner of Canada 2009), Reduce Your Roaming Risks (BMO 2006)

bureaus in the remaining states have offered the same capabilities (Consumers Union, 2008). Eisenstein (2007) demonstrated that implementing credit freezes should basically eliminate new account fraud but the failure of consumers to take full advantage of this capability has meant that new account fraud continues largely undiminished. Carelessness or lack of attention leaves consumers vulnerable.

In summary, identity theft and fraud are significant and growing problems to both individual victims and society at large. Indications are that the problems will continue to grow unless actions are taken. While governments and business have vital roles to play in preventing and deterring identity crime, individuals also play a key role. Even when they are aware of their vulnerabilities and know what to do to minimize them, consumers do not always act in their own best interests. Understanding why consumers behave the way they do in preventing identity theft and detecting identity fraud is therefore key to creating programs to minimize exposure and potential loss. Finding the underlying beliefs and attitudes that motivate these behaviours is the overall objective of this research.

The objective of this research, then, is to understand the behaviour of individuals as they seek to prevent identity theft and detect identity fraud, that is, to develop models which tie together beliefs, attitudes, and intentions to behaviour. Such models would add theoretical insight to consumer identity theft behaviour and prove useful to practitioners seeking to encourage appropriate consumer behaviours. The models will be based on the Theory of Planned Behaviour (TPB) and Protection Motivation Theory (PMT). As suggested by Weinstein (1993) and outlined in Chapter 3 in a comparison of theories, the constructs for TPB and PMT are similar enough that the same source data can be used with both theories. A secondary objective then is to determine which of the two theories is more appropriate to model identity theft prevention and identity fraud detection behaviours, an approach advocated by Weinstein (1993).

Chapter 2 gives background information, including definitions and a review of the literature on identity theft behaviours. Chapter 3 provides a brief description of the theories used and their application to this research. Chapter 4 describes the methods used. Since there are many groups of results, results and discussion are combined in Chapters 5 through 9 so that discussion can be closely related to the associated results. Limitations, further research and conclusions are in the final Chapter 10.

Chapter 2. Background

Perhaps the most rigorous definitions of identity theft and identity fraud were researched by Sproule and Archer (2007). Briefly, identity theft is unauthorized access to personal information or documents and identity fraud is a crime involving the use of a false identity[4]. Identity crime usually occurs in three stages: acquisition (identity theft), use (identity fraud) and discovery. Note that identity theft may be accomplished by legal means; identity fraud is always illegal. Evidence suggests that the longer it takes to discover the theft, the greater the loss and the lower the prospects of apprehension and prosecution of the criminal(s) (Newman and McNally, 2007).

Identity theft occurs in many modes. Koops et al. (2009) list 17 classes of 'attack' designed to yield identity information. Among these are 'traditional' methods such as 'dumpster diving' or stealing credit cards, and 'digital' methods such as retrieving information from discarded hard drives or 'phishing' attacks. Note that only two of the classes ('physical or logical attacks on or by the service provider’s staff' and 'attack(s) on the service provider's data store') numerically account for most identity thefts.

Identity fraud may be classified in two groups: financial and non-financial. Financial identity fraud is possible in an environment in which sellers provide goods and services to strangers for the promise of payment. The trust of the seller is bolstered by information that links the buyer to a specific account or credit history. Financial identity fraud may be classified in three sub-groups: new account, existing account and synthetic identity (see Table 1). New account fraud involves collecting enough personal information about a single individual to enable the perpetrator to effectively impersonate the victim and open new accounts, which the perpetrator then uses to obtain goods and services without ever paying for them, and the victim typically

[4] As noted in Chapter 1, legal definitions vary based on jurisdiction. For example, in Canada, Bill S-4, An Act to amend the Criminal Code (identity theft and related misconduct) which came into force in January 2010, defines identity theft as 'obtaining and possessing identity information with the intent to use the information deceptively, dishonestly, or fraudulently in the commission of a crime' (Department of Justice, 2010). For a compendium of definitions see Jamieson et al., 2012.

learns about the fraud when collection actions are initiated by creditors. Existing account fraud entails the collection of information about an existing account or credit relationship, which the perpetrator then uses illegally and the fraud is usually discovered when unexpected items appear on a bank or credit card statement. Synthetic identities are created when real information, possibly from multiple individuals, is combined with fictitious information to create a new fake identity. This is then used in the same fashion as new account fraud but with the distinction that detection may be much more difficult (Schreft, 2007). By one estimate, up to 80% of all new account fraud involves synthetic identities (Coggeshall, 2007). Non-financial fraud involves the illegal use of a false identity for non-financial crimes. The classic case is to provide a false identity when the perpetrator is arrested for other crimes. Note that the theft of a few pieces of 'non-sensitive' information is not inconsequential. Even mundane information such as name, address and phone number can be used to put individuals at risk (Funk, 2007).

Table 1- Taxonomy of Identity Fraud

Fraud Group	Fraud Sub-Group	Brief Description
Financial	New Account	Create new account for existing person
	Existing Account	Use an existing account for an existing person
	Synthetic	Create new account for synthetic person
Non-Financial		Use fraudulent identity for non-financial crime

There is some discussion as to whether credit card theft and subsequent fraud should be considered 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 (Furleti and Smith, 2005, Sproule and Archer, 2008).

Preventing identity fraud relies on three classes of techniques to ensure that the individual proves who he or she claims to be: token-based, biometrics and knowledge-based (Anderson et al., 2008). Token-based approaches rely on a physical object in the possession of the individual (credit cards are an example). Identity cards have been tried as a way to minimize some forms of identity fraud such as credit card fraud. In practice, improvement has been minimal and costs in both monetary terms and the loss of privacy have outweighed the benefits (Jackson and Ligerwood, 2006). Biometrics use a physical characteristic unique to the individual such as a fingerprint or signature. Ultimately, biometric measures may make identity theft more difficult but the current state of the art has reliability and cost constraints. Even if these technical and commercial problems were solved, there are inherent issues of universality, distinctiveness, permanence, collectability, performance, acceptability and resistance to circumvention in the various biometric technologies (Institute for Prospective Technological Studies, 2005). Although biometric traits may be unique to individuals, biometric identification technologies are susceptible to forgeries and disguises (Chollet et al., 2012). Furthermore, technical measures are not always applicable. Biometric scanning at an Automated Teller Machine (ATM) will not prevent criminals from retrieving personal information from the trash (also known as 'dumpster diving'). The primary knowledge-based technique is the use of passwords, which has also been shown to be problematic (Sasse, Brostoff and Weirich, 2001).

While ideally identity theft and identity fraud should be prevented completely, the costs of doing so both financially and indirectly (such as restraint of commerce) are prohibitive (Anderson et al., 2008). An additional objective then becomes limiting the damage of identity fraud when it does occur. A key to minimizing loss is the quick discovery of the fraud. Losses of more than $5,000 occur in only 10% of cases when the fraud is discovered in less than six months but 30% of cases when discovery takes more than six months.

Despite the importance of the role of consumers and significant survey work, there has been little analytical work done on the behaviours 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 that 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 predicted the level of identity fraud but only for 'new account' fraud. Jamieson, Winchester and Smith (2007) proposed a model of enterprise fraud management. Shareef and Kumer (2012) created a framework of prevention/control measures for organizations. While useful, none of these ‘macro’ models address the behaviours of consumers except as an aggregate. 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; Bowie and Jamal, 2006), behaviour in the online environment (Milne, Rohm and Bahl, 2004), and behaviour to avoid phishing attacks (Arachchilage and Love, 2013). These ‘micro’ models are not comprehensive with respect to consumer identity theft prevention or identity fraud detection behaviours. Milne, Labrecque and Cromer (2009) grouped 49 behaviours into protective and risky groupings and used Protection Motivation Theory (PMT) to model consumer behaviour. Their study, however, concerned online behaviours only and was directed as much at privacy and security as at identity theft[5].

There is a significant amount of research into behaviour in the related area of online security. Lee, Larose and Rifon (2008) applied PMT (Rogers, 1975) to online protection but did not focus specifically on identity theft and did not explore the underlying belief structures. Ng, Kankanhalli and Xu (2009), using a modified version of PMT, did, however, explore the underlying belief structures but in a corporate setting involving only e-mail. Dinev et al (2009) tested a model in two distinct cultures but limited to online spyware protection. Anderson and Agarwal (2010) developed and empirically tested a more comprehensive model of ‘safe

[5] For example, one of the behaviours classified as risky was meeting someone in real life after meeting him or her first online.

computing’ behaviour, also based on PMT. These studies did not specifically explore identity theft or include offline behaviours, and usually examined behaviours within organizational settings only.

The best effort to date to create and validate a comprehensive model of consumer behaviour that prevents and detects identity theft appears to be that of Lai et al. (2012). Their model is loosely based on PMT but leaves out some key constructs, treats 'conventional' behaviours such as shredding documents as exogenous variables, and does not explore the underlying belief structures that influence the cognitive processes that shape behaviour. At the risk of over-generalization, their model can be said to be more organized around whether behaviours prevent victimization rather than explaining behaviour.

Online searches in EBSCO Business Source Complete and Web of Science for the terms 'identity theft' or 'identity fraud' in the subject terms field revealed no other research with models of consumer behaviour. There appear to be no comprehensive theoretical models proposed for the behaviour of consumers in preventing identity theft and mitigating the effects of identity fraud. This is perhaps understandable since behaviours to prevent identity theft and detect identity fraud encompass a wide repertoire of conduct. An analogy would be to create a comprehensive model of behaviours to maintain good health which would need to encompass diet, exercise, and avoiding germs and using other sanitary measures. Each of these encompasses multiple behaviours. So it is with identity protection. Physical security (e.g., shredding documents), password security (e.g., using hard-to break passwords), monitoring accounts (e.g., checking credit card statements) and avoiding risky behaviours (e.g., giving out personal information over the phone), and other behaviours are all necessary to minimize the risk of being the victim of identity theft and maximizing the probability of detecting identity fraud. A comprehensive model is a challenge, yet without a good understanding of the motives behind consumers’ behaviours, programs to promote these behaviours may be ineffective and problems will continue. This thesis explores the relationships between consumer beliefs, attitudes and behaviours in relation to identity theft and fraud prevention and detection. Discovering and understanding the determinants of consumer identity theft behaviours can lead to the design of interventions to improve behaviour by influencing one or more of the determinants. “Security designers must identify the causes of undesirable user behaviour, and address these to design effective security systems” (Sasse, Brostoff and Weirich, 2001).

Chapter 3. Theory

Unlike many harm prevention behaviours, identity theft prevention and detection encompass a wide variety of actions. While protection from lung cancer may be dramatically improved by the single behaviour of quitting smoking, preventing identity theft and detecting identity fraud require a variety of physical measures (e.g., keeping a locked mail box, shredding confidential documents, guarding credit cards), online measures (e.g., using secure passwords, changing passwords frequently, using and keeping up-to-date anti-virus software, avoiding 'click-through' on e-mail) and detection measures (e.g., monitoring credit and bank account activity, regularly checking individual records at credit bureaus, periodically checking the land registry). Gilbert and Archer (2012) reduced these disparate behaviours to a set of five almost orthogonal principal components: using physical security, employing password security, monitoring accounts, monitoring agencies, and avoiding risky behaviours. It is these five components that are the dependent behavioural variables in this research.

Few researchers have grouped consumer identity theft and fraud behaviours using principal components analysis or used expectation-value theories to model these behaviours, as has been done in this thesis. This research focuses on consumer behaviours that are specific to preventing identity theft and detecting identity fraud, and includes offline as well as online behaviours.

The social-cognitive class of theories was chosen as they are widely supported and provide a crucial foundation for creating interventions to change behaviour. As Conner and Norman (2005) state:

> "A significant proportion of social psychology over the past quarter century has started from the assumption that behaviour is best understood as a function of people's perception of reality, rather than as a function of an objective description of the stimulus environment. The question of which cognitions are important in predicting behaviour has been the focus of a great deal of research. This 'social cognitive' approach to the person as a thinking organism has been dominant in social psychology for the past decade or more. ... The focus here is on self-regulation processes and how various social cognitive processes relate to

> behaviour. ... these models provide an important basis for achieving the aim of changing behaviour by providing a means for identifying appropriate targets for intervention work."

The Technology Acceptance Model (TAM) (Davis 1989), popular in the information systems literature, can be said to be in the social-cognitive class since it is based on beliefs (specifically the ease of use and usefulness).

The two theories to explain individual behaviour proposed as the basis for this research are the Theory of Planned Behaviour (TPB) (Ajzen, 2005) and Protection Motivation Theory (PMT) (Rogers, 1983). TPB is a general model that may be applied to a variety of behaviours, including identity theft prevention and identity fraud detection behaviours, whereas other social-cognitive models have been designed for health behaviours. PMT was originally developed for health behaviours involving patient actions to lessen the likelihood of severe health consequences; for example, regular exercise to reduce the chance of coronary heart disease (Milne et al., 2002). The typical application of PMT is analogous to identity theft prevention and identity fraud detection, where the probability of being a victim and the consequences once victimized may be reduced through individual behaviours.

TPB and PMT attempt to explain individuals' behaviours based on their beliefs. Both assume that the anticipation of a negative outcome and the desire to avoid this outcome or reduce its consequences will motivate individuals to undertake preventative behaviours. Beliefs about the severity and likelihood of the outcome, beliefs in the effectiveness of the behaviours, assessments of the capacity to perform the behaviours, and social pressures to undertake defensive behaviours are held to be factors that ultimately influence the intentions to perform behaviours and their actual performance.

Both TPB and PMT have been used extensively in modelling protection behaviours and comparing them was advocated by Weinstein (1993). Both may be said to be in the expectancy-value class of behavioural theories, which posit that individuals hold beliefs about the consequences of their actions and the personal value of those consequences, and act to maximize that value (Fishbein, 1963). This class of theory holds that, while individuals may not be rational in their behaviours, their actions are consistent with their beliefs. Both theories embrace the concept of behaviour following intention: individuals are inclined to behave as they intend to. Intention acts as a mediating variable before actual behaviour. While both theories have separate and distinctive features, there are many similarities as well. Both are extensively described in the literature (Ajzen, 2005; Norman, Boer and Seydel, 2005). The description included in the following discussion will cover only the prominent features of both theories.

3.1 Theory of Planned Behaviour

The Theory of Planned Behaviour (TPB) is a development of the earlier Theory of Reasoned Action (Ajzen and Fishbein, 1980). A diagram of the TPB is depicted in Figure 3.

TPB proposes that intention is influenced by three factors: attitudes, subjective norms, and perceived behavioural control. Attitudes are the individual's overall personal evaluations of the outcomes of performing a behaviour. Subjective norms are the perceptions that individuals hold about how significant others view their performance of the behaviour. Perceived behavioural controls are the opinions that individuals hold about their ability to perform the behaviour. Each of the three contributors to intention is preceded by a set of beliefs: behavioural beliefs create favourable or unfavourable attitudes toward the behaviour; normative beliefs give rise to subjective norms; control beliefs result in perceived behavioural control. Each set of beliefs

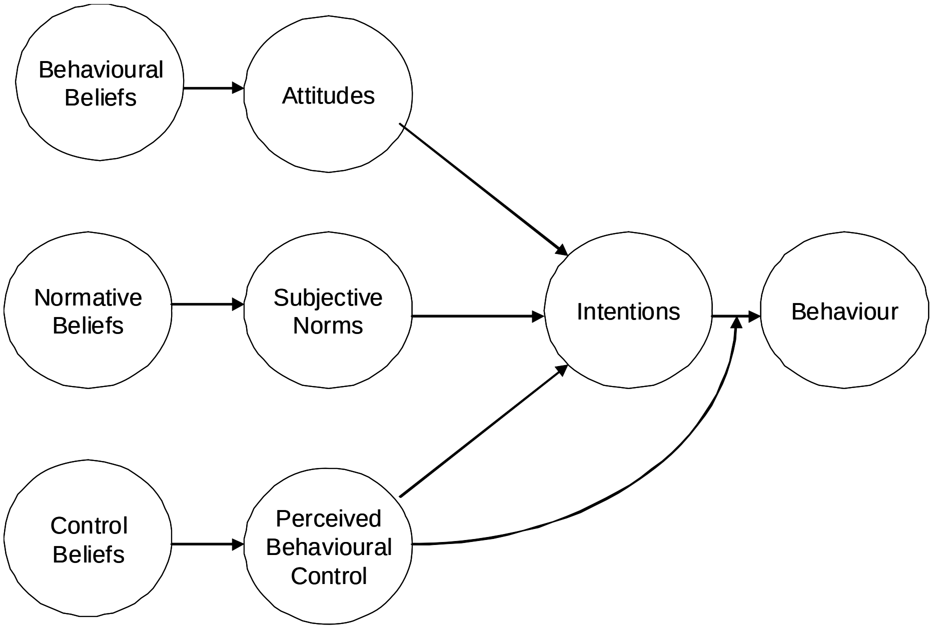


Figure 3 – Theory of Planned Behaviour (Adapted from Ajzen, 2009b)

contains pairs of elements that are multiplied together and the resulting products are summed to obtain an aggregate belief. Behavioural belief pairs consist of the strength of the belief in the outcome of the behaviour and the value of that outcome to the individual. Normative belief pairs include perceptions that significant others favour the individual performing the behaviour and the strength of the individual's inclination to follow the wishes of those others. Control belief pairs include the help or hindrance of an external factor in performing the behaviour and the perception of the likelihood of that external factor arising.

In symbolic terms:

$$\text{Attitude} \propto \Sigma b_i e_i$$

where b_i is the strength of the belief that outcome i will occur and e_i is the value of that outcome to the individual.

$$\text{Subjective Norm} \propto \Sigma n_i m_i$$

where n_i is the strength of the belief that referent i favours the individual performing the behaviour and m_i is the inclination of the individual to comply with the wishes of the referent.

$$\text{Perceived Behavioural Control} \propto \Sigma c_i p_i$$

where c_i is the strength of the belief that factor *i* will occur and p_i is the perceived power of factor *i* to impede or facilitate the performance of the behaviour.

Ajzen (2005, Chapter 4) and before that Ajzen and Fishbein (1980, p34) stress that behaviours described in the beliefs, attitudes, intentions, and performance should be consistent in action, target, context, and time. They suggest, for example, that measuring general personality traits or general beliefs such as conservatism cannot provide accurate insights into how someone will vote in the next election. To achieve this consistency, continuing the example, the behaviour would need to be ‘voting for candidate X in the next election’, the measured intention would need to be ‘vote for candidate X in the next election’, and the attitudes, subjective norms and perceived behavioural control, as well as the beliefs that form the foundation of the attitudes, subjective norms and perceived behavioural control would also be based on ‘voting for candidate X in the next election’. Note that the intentions, attitudes and beliefs would ideally be measured just before the election to ensure that all elements were in the same time context.

Ajzen rejects the influence of other factors such as demographics, personal aspects (values, personality traits, emotions, etc.) and information, except as they affect the belief system in TPB, referring to them as ‘background factors’ (2005, p134).

TPB is a theory applicable to many behaviours. Some applications of the theory are attending class (Ajzen and Madden 1986), buying stocks (East 1993), physical exercise (Courneya, 1995), donating blood (Giles and Cairns, 1995), recycling glass (Lüdemann, 1997), using cannabis (Conner and McMillan, 1999), hunting (Hrubes et al., 2001), dropping out of school (Davis et al., 2002), and contributing to a scholarship fund (Ajzen et al., 2004). TPB must be tailored to each application, since belief structures are specific to each context.

3.2 Protection Motivation Theory

Protection Motivation Theory (PMT) was originally developed by Rogers (1975) to model ‘fear’ interventions in health applications such as quitting smoking, taking medication, and preventing the spread of sexually transmitted diseases. He further developed the theory to include more factors (Rogers, 1983). The theory has since been applied to many other situations outside of the health field. A diagram of the theory appears in Figure 4.

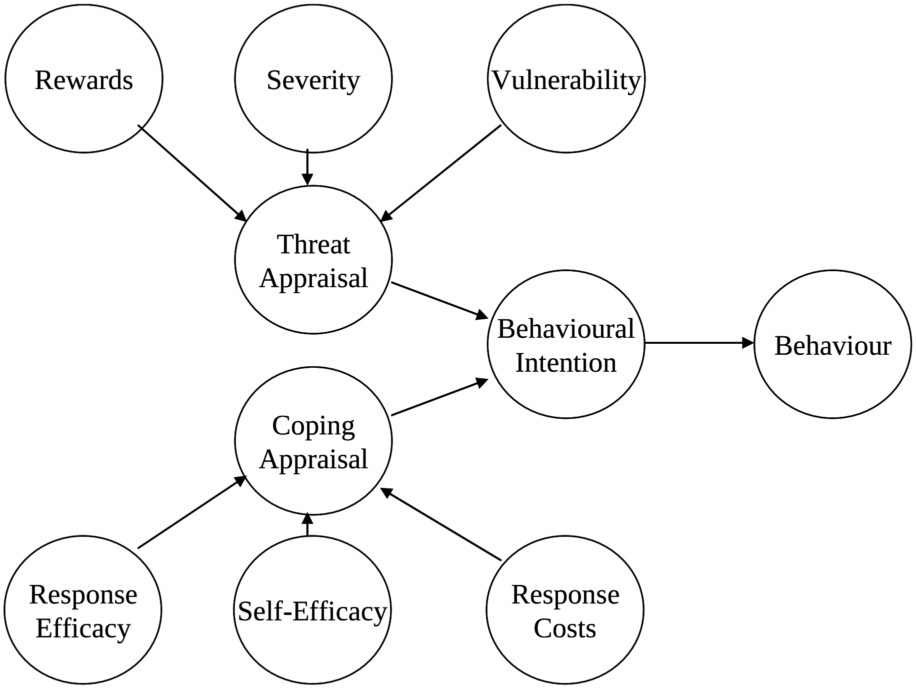


Figure 4 - Protection Motivation Theory (Adapted from Rogers, 1983)

PMT attempts to predict behaviour in the presence of a threat and a suggested behaviour to cope with that threat. The theory holds that the threat and the coping behaviour are assessed separately and are combined to form the behavioural intention (protection motivation). The appraisal of the threat is composed of the intrinsic and extrinsic rewards offset by the severity and probability of the consequences. The coping behaviour is assessed as the effectiveness of the behaviour in counteracting the threat and the ease of performing the behaviour offset by the 'costs' of performing it. Rogers went to great lengths to distinguish the physiological response (fear) from the cognitive response (protection motivation). The classic example of the application of PMT is the cessation of smoking. The intrinsic rewards of smoking (e.g., regulating weight, 'calming of nerves') added to the extrinsic rewards (e.g., social approval) are counterbalanced by the potential severe consequences (medical conditions such as lung cancer, heart attack and stroke) and the increased vulnerability to these consequences. The suggested coping mechanism is to stop smoking, which has been shown to be effective (response efficacy) but which suffers from the fact that smokers have great difficulty in quitting (self-efficacy). Costs may be related to ‘withdrawal’ symptoms. Abraham et al. (1994) state that "the conceptual distinction between the reward value of a risk behaviour and cost of a preventative measure may not be clear." A reward of the threat behaviour may usually be modeled as a cost of the coping appraisal. The rewards of smoking are lost if smoking ceases. In most applications of the theory, rewards are not explicitly modeled but are incorporated into response costs (Norman, Boer and Seydel, 2005).

While PMT is not as general as TPB and has typically been applied in health situations, it may be and has been used in a variety of applications such as fear and prevention of nuclear war (Allen, 1993; Wolf, Gregory and Stephan, 1986), adoption of anti-plagiarism software (Lee, 2011), driver education (Griffeth and Rogers, 1976), problem gambling (Munoz, Chebat and Suissa, 2010), energy consumption (Hass, Bagley and Rogers, 1975), compliance with security policy (Herath and Rao, 2009), surveillance and justice perception (Workman, 2009), appeals to help (Shelton and Rogers, 1981), and (closer to identity theft) online information security (Johnston and Warkentin, 2010).

3.3 Theory Comparison

While on the surface TPB and PMT look quite different, in reality they both use similar constructs connected in similar ways. Weinstein (1993) compared four theories of health protection behaviour including PMT and the Theory of Reasoned Action (the predecessor of TPB). Both theories generally use the same (albeit differently named) independent variables (see Figure 5). The belief strength of TPB is similar to vulnerability in PMT in that they both measure the subjective probability of the consequences of the behaviour. Outcome evaluations in TPB are the perceived consequences of the behaviour, including the severity, costs, and ability to prevent adverse consequences (called response efficacy in PMT). In its original form, PMT does not explicitly model social pressures as TPB does in its normative beliefs, but it potentially includes them as one of the response costs and has been extended to include ‘social norms’ (Tanner et al., 1991). The control beliefs of TPB are essentially the same as the self-efficacy of PMT. Both theories result in a behavioural intention construct, which both view as a predictor of behaviour.

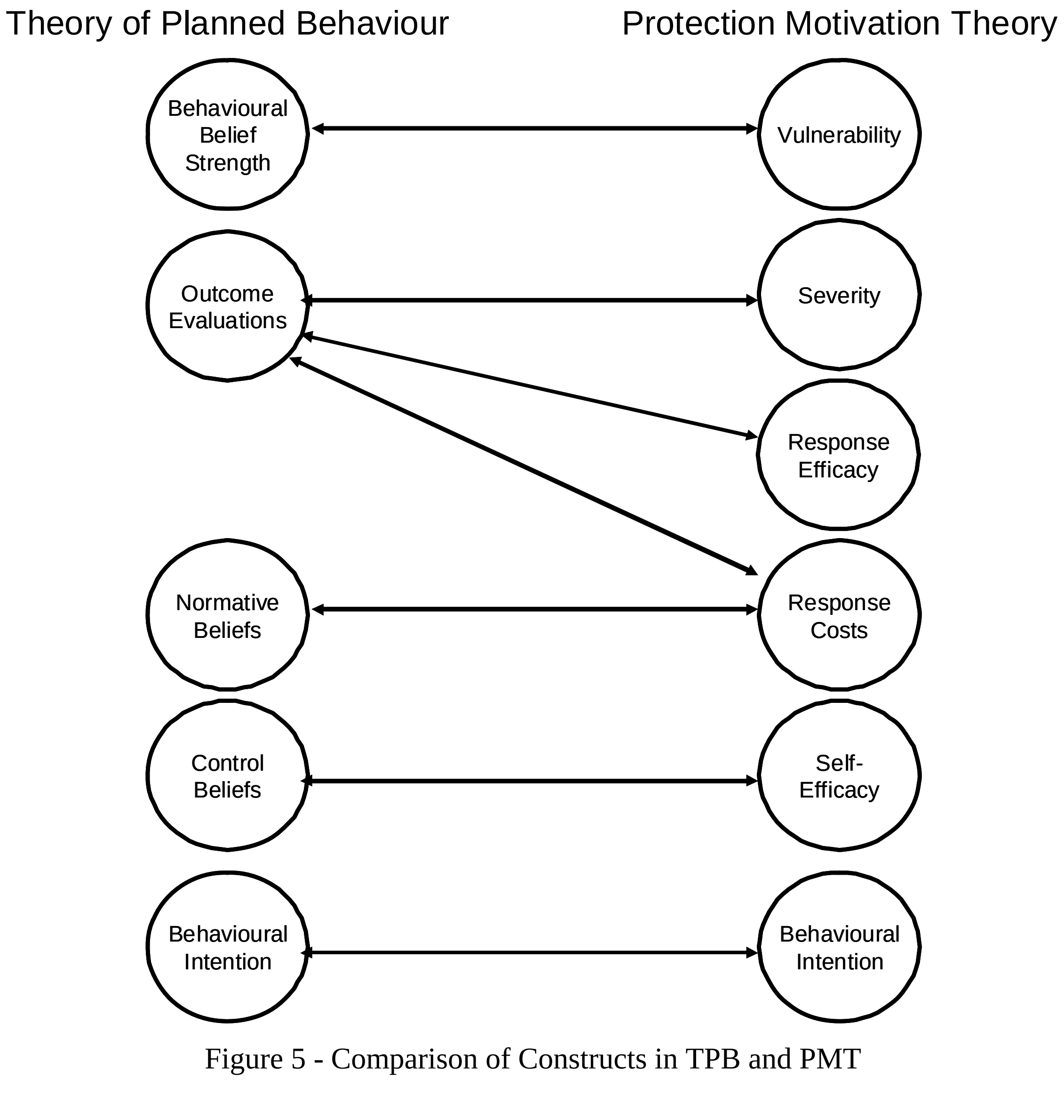


Figure 5 - Comparison of Constructs in TPB and PMT

The primary differences between TPB and PMT lie in the way the independent variables are combined to model intention. TPB uses a linear sum of the three primary variables (attitude, subjective norm and perceived behavioural control), with the weights to be determined experimentally. Rogers is less definitive for PMT. He raises the possibility of non-linear relations and suggests that, in some cases, the response may be an inverted U shape. If self-efficacy is low and/or the response efficacy is low relative to the threat appraisal, individuals may engage in ‘maladaptive coping responses’ that reduce fear without dealing with the threat. Such responses include denial, avoidance (e.g., not thinking about adverse consequences), wishful thinking (e.g., believing that circumstances will change and the threat will disappear) and fatalism (e.g., outcomes are in the hands of fate and not subject to personal action) (Ben-Ahron, White and Phillips, 1995). These maladaptive responses may result in actually increasing undesirable behaviour instead of decreasing it (Rippetoe and Rogers, 1987). If smokers, for example, believe that they cannot quit smoking (low self-efficacy), they may ignore the threat and actually increase their use of tobacco products (Plotnikoff and Trinh, 2010). PMT makes no prescriptions about consistency in action, target, context or time, as does TPB, but meta-analyses have shown that the relation between protection motivation (intention) and behaviour weakens as the time between them lengthens (Floyd et al., 2000; Milne et al., 2000).

Note that neither theory can be applied without customization to the application. TPB requires that salient[6] beliefs be ascertained, typically with a small sample of individuals (20-30) using qualitative methods (often either a survey with free-form responses or a focus group) and the results used to construct the final instrument (Ajzen and Fishbein, 1980, Chapter 6). Similarly, it is suggested for PMT that preliminary semi-structured interviews be conducted with a small sample to elicit salient beliefs about the threat and suggested coping behaviour under study (Norman et al., 2005).

3.4 Application of Theories to Identity Theft Prevention and Identity Fraud Detection

Both TPB and PMT may be applied to identity theft prevention and identity fraud detection behaviours. As noted previously, Gilbert and Archer (2012) identified five principal components

[6] In order to distinguish between prominent and statistically significant, throughout this document the term 'significant' will imply statistical significance, while the term 'salient' will be used to mean important but not necessarily statistically significant.

to behaviours based on an online study of a structured sample of 3,016 individuals in Canada. Using principal components analysis with oblimin oblique rotation, the components and associated behaviours were interpreted as:

1. Monitoring Accounts
   I monitor bank account balances and activity
   I monitor credit card accounts and activity

2. Monitoring Agencies
   I request a copy of my credit report
   I check Land Registry Office records to ensure validity of ownership

3. Using Password Security
   I have different passwords for different applications or services
   I use hard-to-break passwords (i.e. avoid using family members' names or common dictionary words, and include special characters and numbers in passwords)

4. Using Physical Security
   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

5. Avoiding Risky Behaviours (reverse-coded)
   I give personal information over the phone to people who claim to do surveys, or people offering products or services at special prices
   I respond to a business by clicking on a link in an e-mail
   I select "remember my card number" or "remember my password" for online log-ins

Of particular interest is the lack of correlation among the components. The maximum correlation is .20, so the components are almost orthogonal. Consumers seem to 'buy in' to one form of identity theft prevention or detection but ignore others (Gilbert and Archer, 2012). Given this minimal correlation, it is appropriate to treat each component as a separate behaviour in both TPB and PMT theories. Each behavioural component is a formative construct of the constituent behaviours; for example, the physical security component is composed of the following behaviours: using a locked mailbox, shredding unwanted confidential documents, and keeping confidential documents locked up. The treatment of multiple behaviours in a single analysis is similar to a study that used TPB for weight loss, which also included multiple behaviours (Ajzen and Fishbein, 1980, Chapter 9).

In line with the overall objective of finding the underlying beliefs and attitudes that motivate identity theft prevention and detection behaviours, and considering the TPB and PMT theories, the research in this thesis addresses the following seven research questions:

1) What are the salient consumer beliefs about the consequences and outcomes of identity theft prevention and identity fraud detection behaviours that influence attitudes toward behaviours and, in turn, intentions to perform the behaviours?

2) What are the consumer beliefs about factors that help or hinder performance of identity theft prevention and identity fraud detection behaviours that influence perceptions of the ability to perform the behaviours and, in turn, intentions to perform the behaviours?

3) What are the consumer beliefs about the influence of significant others toward performance of identity theft prevention and identity fraud detection behaviours that affect inclination to perform behaviours and in turn intentions to perform the behaviours?

4) Do attitudes and beliefs toward some identity theft prevention and identity fraud detection behaviours affect the intention to perform other identity theft prevention and identity fraud detection behaviours?

5) Do consumer beliefs about the consequences and outcomes of identity fraud in general influence attitudes toward specific behaviours and, in turn, intentions to perform the behaviours?

6) Which of two theories, Theory of Planned Behaviour (TPB) or Protection Motivation Theory (PMT), better models consumer identity theft prevention and identity fraud detection behaviours?

7) Do consumers consider credit card fraud less threatening than other identity fraud?

Since one of the objectives of this research is to determine which of the two theories is more appropriate to model identity theft prevention and identity fraud detection behaviours, to fairly compare the two theories, the application of both has been kept as close as possible to the tenets of each theory. The application of TPB to identity theft prevention and identity fraud detection behaviours is shown in Figure 6.

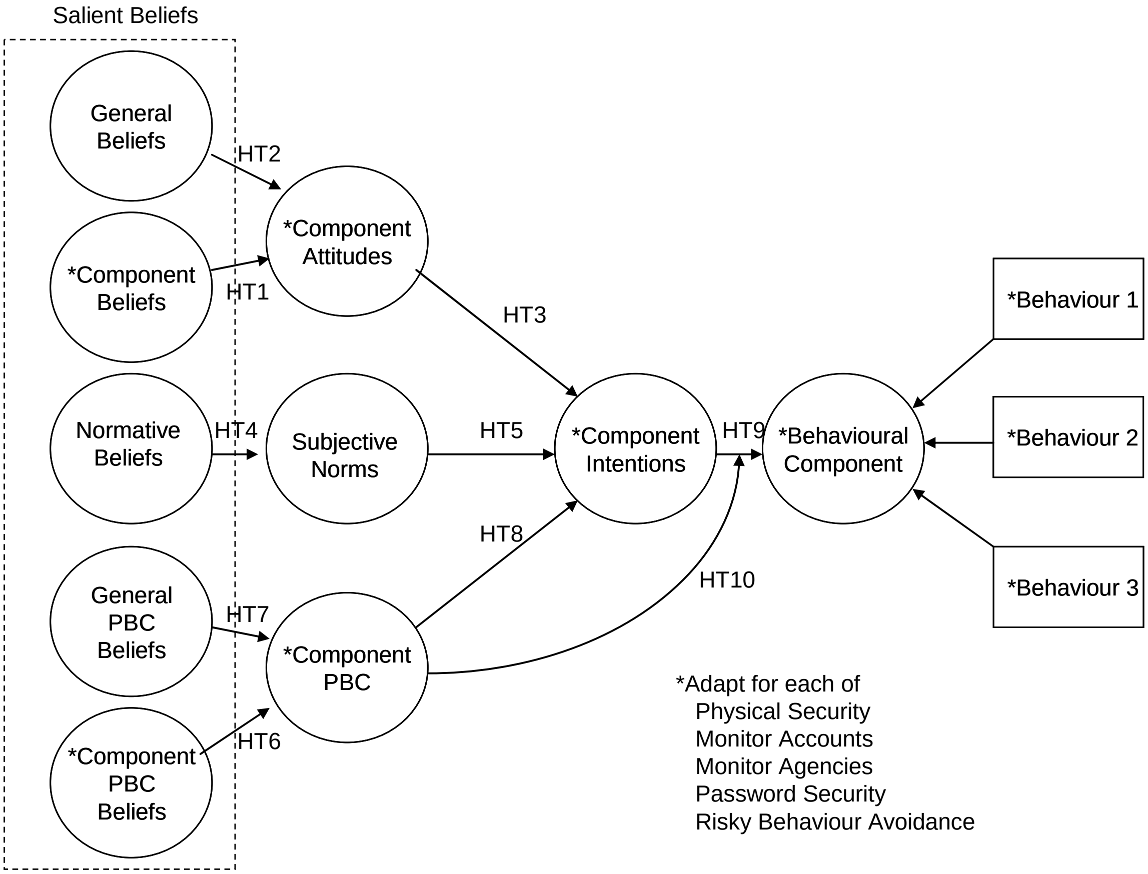


Figure 6 – Theory of Planned Behaviour Applied to Identity Theft Behaviours

The multi-faceted behaviours associated with identity theft prevention and detection suggest a breakdown of the belief structures proposed in TPB. The individual behavioural components may be considered to be influenced by two classes of beliefs: those specific to the behavioural component and those about identity theft prevention and detection in general. Each behavioural component has consequences beyond identity theft, and beliefs about those other consequences will influence the attitudes and subsequent intentions and behaviours. Attitudes are therefore influenced by both the beliefs about the behavioural component and the beliefs about identity theft in general. For example, individuals may believe that giving out personal information over the phone may carry the risk of identity theft but may also lead to getting better ‘deals’. The decision to undertake the behaviour will be the result of balancing the beliefs about the benefits of the behaviour with the beliefs about the risk of identity theft. This gives rise to:

TPB Hypothesis 1 (HT1): *An individual’s beliefs specific to a behavioural component positively affects attitudes toward that behavioural component.*

TPB Hypothesis 2 (HT2): *An individual’s beliefs about identity theft in general influence*[7] *attitudes toward all behavioural components.*

In line with TPB:

TPB Hypothesis 3 (HT3): *An individual’s attitudes toward a behaviour component positively affect the intention to perform the component behaviours.*

Subjective norm is treated in the model in general rather than specific to each behavioural component. Of the three antecedents of behavioural intention in TPB, subjective norm is generally the least predictive (Armitage and Conner, 2001). It tends to be less significant when behaviours are performed in private (Boss et al., 2008) as most identity theft prevention and detection behaviours are. Subjective norm has been shown to be an insignificant predictor in the intention to adopt anti-spyware software (Lee and Kozar, 2005). There is, on the other hand,

[7] It is not possible to define the direction of the influence in general because some studied behaviours reduce the likelihood of identity theft and some increase it. For direction of influence, see Table 1.

evidence that subjective norm has significant influence on the intention to comply with security policies in organizational settings (Bulgurcu, Cavusoglu and Benbasat, 2010). These findings suggest that normative beliefs and subjective norm are effective when applied at the general level (compliance with a policy) but weak when applied to detailed components of that policy (adoption of anti-spyware). In line with these results, and in the interests of parsimony, normative beliefs and subjective norm have been included at the general level only. The following are proposed:

TPB Hypothesis 4 (HT4): *An individual's normative beliefs about identity theft positively affect the individual's subjective norm.*

TPB Hypothesis 5 (HT5): *An individual's subjective norm positively influences the intention to perform identity theft prevention and detection behaviours.*

Similar to the behavioural beliefs, there are general and specific aspects to control beliefs. One would expect, for example, that lack of knowledge about identity theft in general would have an influence on the intention to perform all behavioural components. The perceived behavioural control and associated beliefs, however, are more likely to be tied to specific behaviours. The control aspects are in the 'nitty-gritty' of actually performing the behaviours. This dominance of control beliefs specific to behaviours (as opposed to identity theft in general) is borne out by the results of the exploratory study, where there were only four general control beliefs and 30 control beliefs specific to behaviours. The following hypotheses are formed:

TPB Hypothesis 6 (HT6): *An individual's control beliefs specific to a behavioural component positively affect perceived behavioural control toward that behavioural component.*

TPB Hypothesis 7 (HT7): *An individual's control beliefs about identity theft in general influence perceived behavioural control toward all behavioural components.*

TPB Hypothesis 8 (HT8): *An individual's perceived behavioural control of a given behavioural component positively affects the intention to perform component behaviours.*

Following TPB, these final hypotheses are proposed:

TPB Hypothesis 9 (HT9): *An individual's intention to perform component behaviours positively affects the actual performance of the component behaviours.*

TPB Hypothesis 10 (HT10): *An individual's perceived behavioural control of a specific behavioural component moderates the influence of the intention to perform component behaviours on the actual performance of the component behaviours.*

The alternative theory involving the application of PMT to identity theft prevention and identity fraud detection behaviours is shown in Figure 7.

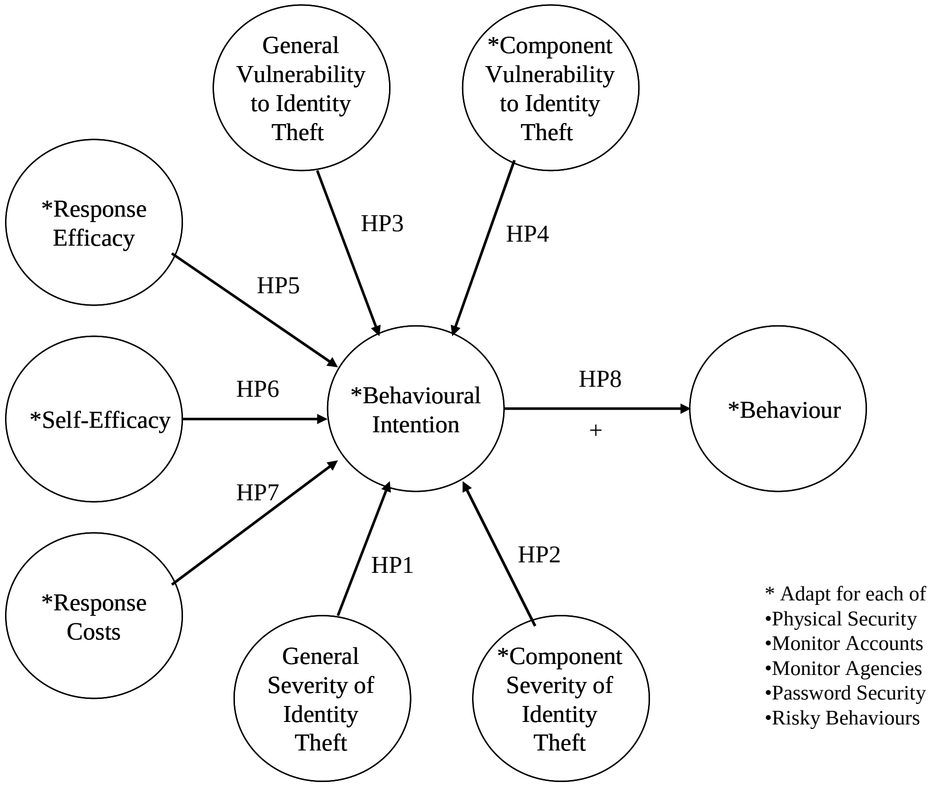


Figure 7 – Protection Motivation Theory Applied to Identity Theft Behaviours

In practice, the threat appraisal and coping appraisal constructs postulated in PMT are difficult to measure directly and are usually excluded in practice, with each of their precursors modeled to directly affect behavioural intention (Norman, Boer and Seydel, 2005). As in TPB, the behavioural intention and behaviour are the five principal components identified by Gilbert and

Archer (2012) (physical security, monitoring accounts, monitoring agencies, password security, and risky behaviours). Extrinsic and intrinsic rewards are included in the response costs (Abraham et al., 1994; Norman, Boer and Seydel, 2005). The component beliefs that are the outcomes and likelihoods of TPB, become the component severity and vulnerability constructs respectively of PMT. As in the case of TPB, the PMT model includes both general and component-specific constructs. The direction of the effects on intention cannot be generalized, since some behaviours prevent or detect identity theft and others, specifically the risky behaviours, make identity theft more likely. In line with PMT, the hypotheses are:

PMT Hypothesis 1 (HP1): *An individual's assessment of the severity of identity theft affects the intention to engage in component behaviours.*

PMT Hypothesis 2 (HP2): *An individual's assessment of the severity of the consequences of component behaviours affects the intention to engage in component behaviours.*

PMT Hypothesis 3 (HP3): *An individual's assessment of his or her vulnerability to identity theft affects the intention to engage in component behaviours.*

PMT Hypothesis 4 (HP4): *An individual's appraisal of his or her vulnerability to the consequences of component behaviours will affect the intention to engage in component behaviours.*

All of the coping appraisal portions of PMT consist of the behaviour-specific components of TPB, since they deal with the assessment of the ability of the behaviour to mitigate the threat of identity theft and fraud. The perceived behavioural control for each behavioural component becomes self-efficacy in PMT. In addition to the TPB reward/cost outcomes, the PMT response costs include the normative elements of TPB. These considerations give rise to the following hypotheses:

PMT Hypothesis 5 (HP5): *An individual's assessment of the response efficacy to counter the threat of identity theft will affect the intention to perform component behaviours.*

PMT Hypothesis 6 (HP6): *An individual's appraisal of their ability to perform the behaviour will affect the intention to perform component behaviours.*

PMT Hypothesis 7 (HP7): *An individual's assessment of the costs of performing the behaviour will affect the intention to perform component behaviours.*

Finally, in line with PMT:

PMT Hypothesis 8 (HP8): *An individual's intention to perform the component behaviours (protection motivation) will positively affect the actual performance of the behaviours.*

Chapter 4. Method

The overall research plan included:

Phase 1 - Exploratory questionnaire

A primarily qualitative instrument to elicit salient beliefs about identity theft prevention and identity fraud detection behaviours from a small convenience sample

Phase 2 -Survey using an Internet survey service

a) Development of a primarily quantitative instrument using beliefs elicited in Phase 1

b) Implementation with 'soft launch' followed by full launch

Ideally, a longitudinal study with control and 'treatment' groups would be the preferred method to survey beliefs at one point and then survey the actual behaviours at a later point to fully test the predictive capabilities of the model. This is problematic for logistical and theoretical reasons. A longitudinal study is difficult to implement in a survey panel, since it requires the same participants at both points in time, which is a challenge. Furthermore, it is unlikely that 'pristine' participants who have not already been exposed to identity theft information and performed at least some of the preventative and detective behaviours can be found.[8] The method chosen for the research was therefore a cross-sectional study, used in each of the steps in the overall research plan.

4.1 Phase 1 - Exploratory Questionnaire

Following the recommendations of Ajzen and Fishbein (1980, Chapter 6) for TPB and Norman, Boer and Seydel (2005) for PMT, an exploratory questionnaire was developed to elicit salient

[8] Some studies using PMT (e.g., new cardiac patients newly encouraged to exercise) or TPB (e.g. voting behaviour when a new slate of candidates is presented for each election) can find participants whose studied behaviours are relatively isolated from previous experience.

beliefs about identity theft prevention and identity fraud detection behaviours (see Appendix A). The qualitative survey method was chosen over focus groups for several reasons. Focus groups tend to use smaller numbers of participants than questionnaires and it was deemed more appropriate to involve a relatively large sample to ensure that all salient beliefs were elicited. From a practical point of view, focus groups take more time to complete for both the participants and the researcher. The instrument in Appendix A is a modification of the template provided by Ajzen (2009) on his website. The modifications tailor the questionnaire to the identity theft context. There were four sets of questions. The first set covered beliefs about identity theft prevention and detection behaviours in general. It is analogous to the TPB study of weight loss behaviours where intentions to diet apply to a wide variety of behaviours (avoiding snacks between meals, cutting down on starchy foods, avoiding situations where one might be tempted to eat too much, decreasing food intake in general and eating on a consistent schedule) that may result in weight loss (Ajzen and Fishbein, 1980, Chapter 9). The second set of questions covered the five principal components from Gilbert and Archer (2012) and was designed to elicit beliefs about specific types of behaviour, such as practising physical security to safeguard confidential and sensitive documents. Preliminary discussions with some users indicated that normative beliefs were not specific to the behavioural components but applied to identity protection in general. To keep the questionnaire to a reasonable size, in line with Hypotheses HT4 and H5 of the TPB, and considering the lack of explicit incorporation of social influence in PMT, normative belief questions were limited to the general section. The last two sections of the questionnaire were quantitative and polled attitudes and previous experience respectively.

4.2 Phase 2- Survey Instrument

Phase 2 used the results of the Phase 1 exploratory questionnaire to develop a primarily quantitative survey as documented in sub-section 4.2.1. The number of items turned out to be very large and required accommodations, as discussed in sub-section 4.2.2. The implementation of the Phase 2 survey is described in sub-section 4.2.3.

4.2.1 Phase 2 Survey Instrument Development

The frequency of the codes developed from the qualitative items in the exploratory questionnaire was used to guide the creation of the Phase 2 (primarily quantitative) instrument. A small number of codes (14 of the 1016) were immediately excluded because they were small in frequency (typically only a single comment) and were deemed irrelevant.[9] The remaining 1,002 codes were grouped into the TPB belief classifications and codes were sorted within class by descending frequency of occurrence. Some codes were dropped from further consideration because they related less to issues that were within the behavioural purview of the individual and more to aspects that would make identity theft less likely. For example, better security on bank machines and at retail checkouts was mentioned by almost half of the respondents and would help to reduce exposure to identity theft but is not within the behavioural repertoire of the individual and so was excluded from the Phase 2 survey.

In general, the remaining codes (Appendix B lists the codes that were kept in the final questionnaire) became pairs of questions in the Phase 2 survey, as specified in TPB. For example, physical security outcomes had the following codes and frequencies: PSO1-Security (9), PSO4-Under personal control (9), PSO2-Loss of identity information (4), and PSO3-Info available for taxes etc. (1). PSO3 was dropped because it was mentioned by only one respondent. The other three codes for physical security outcomes gave rise to the following item pairs:

Maintaining security of my personal financial documents is (extremely bad···[10]extremely good).
If I physically secure my documents, it is (extremely unlikely···extremely likely) that my personal identity information will be secure.

Maintaining personal control of my personal information is (extremely bad···extremely good).
If I physically secure my documents, it is (extremely unlikely···extremely likely) that I will maintain personal control of my identity information

Losing my personal identity information is (extremely bad···extremely good).

[9] For example, one respondent suggested that identity theft could be reduced if all personal identification, (e.g., driver's license, social insurance number, credit card, debit card etc.) was contained on one card.
[10] ··· These are the extreme ends of a 7 point Likert scale.

If I physically secure my documents, it is (extremely unlikely···extremely likely) that I will lose my personal identity information

In one case, in control beliefs, one issue had multiple factors but only one personal impact. The case involved passwords where multiple passwords for different applications, using hard-to-break passwords, having different password standards in different applications, and changing passwords frequently all contributed to making passwords difficult to remember. The solution was to use the same strength factor with multiple power factors; i.e., the strength of the belief that secure passwords were hard to remember was multiplied by each of the power factors (multiple passwords, hard-to-break passwords, differing standards, and frequent changes) to generate four control factors. The other departure from strict application of TPB principles was a few cases in which the belief was that the behaviour had no consequences. For example, some respondents believed that checking the land registry is required only when buying or selling their home. There was no outcome in this case that could be assessed as good or bad. In this case the single probability was used instead of the outcome/probability pair that the theory specifies. Since PMT does not require pairs of questions, these matching considerations did not apply to the PMT model.

Care was taken in the creation of items in the Phase 2 instrument for eliciting attitudes (TPB)/ vulnerabilities (PMT). Weinstein and Nicolich (1993) argue that individuals' current behaviour influences their perception of their vulnerability. If they currently behave in a manner that alleviates the probability of harm, they may understate their vulnerability. The problem is of particular concern in cross-sectional studies, since attitudes/vulnerabilities are measured at the same time as intentions and behaviours. Gilbert and Archer (2012), for example, found no statistically significant difference in identity theft prevention and detection behaviours between those that were 'not at all concerned' and those that were 'extremely concerned' about being victims of identity theft. Apparently, the level of concern was moderated by current behaviours to prevent identity theft. Van der Velde et al. (1996) suggest the use of conditional items for perceived vulnerability (e.g., How likely are you to be the victim of identity theft if you took no precautions to prevent it?) rather than unconditional items (e.g., How likely are you to be the victim of identity theft?) to ensure that the measure of vulnerability is uncontaminated by the effects of current behaviours.

In general, each component was treated as a whole. For example the ‘monitoring accounts’ component, which includes monitoring both bank accounts and credit cards, does not have items specific to either bank accounts or credit cards. There are two exceptions. The ‘risky behaviours’ component contains behaviours that are otherwise unrelated, so a set of questions for each behaviour (using ‘remember my password’, clicking through an Internet link on an e-mail and giving out personal information over the phone) was created. The other exception is the ‘monitoring agencies’ component, which consists of getting a credit report and checking the land registry. The latter only applies if the consumer is a home owner. To accommodate individuals that rent their accommodation, each of the component behaviours was treated separately, with a qualifying question for the home owner section. The final eight groups of questions in the Phase 2 survey are shown in Table 2. Each question group led to a separate analysis. The hypothesized influence of general identity theft beliefs on intention is also shown in Table 2.

Table 2 – Groupings in Quantitative Study

Behaviour Component	**Analysis Group(s)**	**Influence of General Beliefs**
Physical Security	Physical security	+
Monitoring Accounts	Monitoring accounts	+
Monitoring Agencies	Getting credit report Checking land registry	+ +
Password Security	Password security	+
Avoiding Risky Behaviours	Using ‘remember my password’ Giving information over the phone Clicking on link in e-mail	- - -

The survey instrument (primarily quantitative) in Phase 2 consisted of seven sections in three sets (see Table 3). The first set of items (Initial Questions) included demographic and screening questions. The next set included section 2 (General Questions 1 through 10) and incorporated items designed to address behavioural, subjective and control beliefs about identity theft behaviours in general, as well as attitudes, subjective norms, perceived behavioural control, intentions, and self-reported behaviour for each of the eight analysis groups. Also included in the second section were a few open-ended qualitative questions. The third set included the other five sections (Specific Questions 1 through 12) contained items for behavioural and control beliefs for each of the five behavioural components.

Table 3 - Questions in Phase 2 Survey

Set	**Section**	**Questions**	**Contents**
Initial	1		Screening and demographic questions
General	2	1	Outcome evaluations of personal identity information protection
		2	Self-reported behaviours. Includes behaviours for all five components
		3	Direct measures of attitude, subjective norm, perceived behavioural control, and intention. Includes all five behavioural components
		4	Motivation to comply with normative beliefs
		5	Perceived likelihood of outcomes of personal identity information protection
		6	Control beliefs about personal identity information protection
		7	Power of control factors about personal identity information protection
		8	Normative beliefs about personal information protection
		9	PMT questions
		10	Qualitative questions
Specific*	3	1	Physical security outcomes
		2	Physical security likelihoods
	4	3	Password outcomes
		4	Password likelihoods
	5	5	Monitor accounts outcomes
		6	Monitor accounts likelihoods
	6	7	Credit report outcomes
		8	Credit report likelihoods
		9+	Land registry outcomes
		10+	Land registry likelihoods
	7	11	Risky behaviour outcomes
		12	Risky behaviour likelihoods

* Respondents were assigned at random to only one of the specific sections (see section 4.3).

+ Only respondents that owned their homes completed these questions.

The Phase 2 survey is found in Appendix D. The number of items required to ensure statistical validity was a concern and is addressed in the next sub-section (4.2.2). Since the survey instrument was tailored to the identity theft context, a 'soft launch' was run using approximately 10% of the target number of respondents. Responses were scrutinized for major problems before the 'full launch'. The responses from the 'soft launch' were included in the final analysis, since only very minor corrections were made to the instrument before the 'full launch'.

While Ajzen typically used linear regression for TPB analysis, Structured Equation Modeling (SEM) is a second-generation technique that enables investigation of interrelated research hypotheses in a single, systematic and comprehensive analysis (Gefen et al., 2000). Partial-Least-Squares-based SEM (PLS) was used to analyze the results. PLS was chosen for several reasons. First, at least some of the behavioural constructs (e.g., physical security) were formative and can be handled by PLS but not by covariance-based SEM (Chin, 1998). Second, while both TPB and PMT theories are well established, the application to identity theft is new and in that sense can be considered exploratory. Due to the over-fitting tendencies of covariance-based SEM, PLS is preferred for exploratory research (Hair et al., 1998). Finally, many of the distributions of variables in the social sciences are non-normal and some exponentially so (Micceri, 1989). Few of the variables in either of the Phase 1 or Phase 2 surveys were normally distributed (see sub-section 6.1.4). The data distribution assumptions of PLS are less restrictive than those of covariance-based SEM (Anderson and Gerbing, 1988) and more robust against departures from normality (Chin and Newstad, 1999; Gefen et al., 2000). Note that the perceived behavioural control construct of TPB that moderates the interaction between intention and behaviour would until recently have posed problems for covariance-based SEM. Non-linear responses such as those proposed by Rogers (1983) for PMT would traditionally have posed problems for both types of SEM. More recent techniques for covariance-based SEM (Lee, Song and Poon, 2004) and PLS (Henseler and Chin, 2010) have provided new approaches for non-linear models and models with interacting variables, however.

The SEM analytical software for this research was WarpPLS, which handles both moderators and non-linear responses and, as do all PLS implementations, formative variables.

4.2.2 Phase 2 Survey Instrument Development Practical Considerations

The number of items in the Phase 2 survey presents a problem when eight analysis groups are dealt with in a single instrument. In addition to the direct measures for attitudes, subjective norm and PBC, for each of the codes retained from Phase 1 (exploratory questionnaire), according to TPB there should be two items in the Phase 2 (see Table 4 for the counts of items in each section). The total of all the items in every section of a complete survey would be 289. This would result in a very long survey, which could have resulted in a large number of respondents abandoning before completion. As well as the logistical problems it causes, an overly long survey may also have biased the results in that only motivated respondents might have completed the entire instrument. Reducing the number of direct measure items to a single item each could have reduced the total item count by 56 but would have greatly compromised statistical validity. Artificially reducing the number of belief items would have compromised the theoretical foundation and practical utility of the study, since it is the beliefs that are of primary benefit. Demonstrating that individuals intend to do things they have positive attitudes toward is not profound - it is the underlying beliefs that are of most interest.

One possible solution for the overly long survey would have been to simply treat each of the analysis groups as a separate study with completely different surveys. The difficulty with this approach was that it would not permit the study of the impact of one belief set on the attitudes, intentions and behaviours of the other behavioural components. The behaviours may be orthogonal but it does not necessarily follow that the beliefs are as well.

Table 4 - Number of Survey Questions Required

General Questions

Screening	9
Behavioural beliefs	18
Normative beliefs	24
Control beliefs	8
Direct measures	74
Behaviours	12
PMT	11
Qualitative	3
Total	**150**

Physical Security

Behavioural beliefs	8
Control beliefs	10
Total	**18**

Password Security

Behavioural beliefs	10
Control beliefs	9
Total	**19**

Monitoring Accounts

Behavioural beliefs	6
Control beliefs	10
Total	**16**

Monitoring Agencies

Credit Report	
Behavioural beliefs	9
Control beliefs	6
Total	15
Checking land registry	
Behavioural beliefs	9
Control beliefs	6
Total	15
Total Monitoring Agencies	**30**

Risky Behaviours

Using ‘Remember Password’	
Behavioural beliefs	6
Control beliefs	8
Total	14
Personal info over phone	
Behavioural beliefs	11
Control beliefs	6
Total	17
Clink on Link	
Behavioural beliefs	10
Control beliefs	6
Total	16
Total Risky Behaviours	**47**

The strategy to reduce the size of the survey was twofold. The first strategy was to reduce the direct measures from four items per construct to three. Given that there were eight analysis groups and two direct measures (attitude and perceived behavioural control), that reduced the item count by 16 and still left three items for each direct measure. These reductions were included in the survey and the numbers reflected in the ‘general’ counts in Table 4. The second strategy was to split the sample into five equal, randomly selected sub-samples. The constructs for TPB may be classified into a 5 by 2 matrix, with the five rows being the identity theft behavioural components and the two columns being the sections of the TPB model. The first column contains the set of belief constructs (behavioural and control) that are precursors to the 'direct measures' set of constructs in the second column (attitudes, subjective norm, perceived behavioural control, behavioural intention and behaviour) (see Table 5).

Table 5 - TPB Construct Grouping

Behavioural Component	Behaviour-Specific Behavioural Beliefs Behaviour-Specific Control Beliefs	General Identity Theft Beliefs Normative Beliefs Attitudes Subjective Norm (SN) Perceived Behavioural Control (PBC) Behavioural Intention Behaviour
Physical Security	Physical security beliefs	Physical security attitudes, SN, PBC, intention, behaviours
Monitor Accounts	Beliefs about monitoring accounts	Monitoring accounts attitudes, SN, PBC, intention, behaviours
Monitor Agencies	Beliefs about monitoring agencies	Monitoring agencies attitudes, SN, PBC, intention, behaviours
Password Security	Password security beliefs	Password security attitudes, SN, PBC, intention, behaviours
Risky Behaviour Avoidance	Risky behaviour beliefs	Risky behaviour attitudes, SN, PBC, intention, behaviours

Each randomly selected sub-sample was presented with only one of the behavioural sets of belief items corresponding to one of the component behaviours (Appendix D-specific questions) but all sets of direct measures of perceived behavioural control, subjective norm, attitude and intention items, as well as the general identity theft belief items (Appendix D-general questions).

The resulting numbers of items in each sample are shown in Table 6. The minimum number of items to be administered to a sample was 155 and the maximum was 197. The estimated completion time was about 30 minutes depending on which set was presented and the speed of the respondent. Thirty minutes is the maximum time limit suggested by Fowler (2001, p103).

Table 6 - Number of Survey Items in Each Sample

Sample	General	Specific	Total
Physical Security	150	18	168
Password Security	150	19	169
Monitoring Accounts	150	16	166
Monitoring Agencies	150	15-30	155-180
Risky Behaviours	150	47	197

4.2.3 Phase 2- Analysis Methodology

Due to the multiple behaviours being studied and the sub-sampling strategy, the study is more like a series of enquiries rather than a single study. As such, each of Chapters 5 through 9 deals with one aspect of the research and includes both results and discussion. Chapter 5 covers the Phase 1 exploratory survey. Chapter 6 provides the results and discussion using the results from the full sample (see Table 7 with reference to Table 5).

Table 7 - Observations in Sections 6.1 and 6.2

Sample	Beliefs	Others*
Physical Security		✓
Password Security		✓
Monitoring Accounts		✓
Monitoring Agencies		✓
Risky Behaviours		✓

*Attitude, Subjective Norm, Perceived Behavioural Control, Behavioural Intention, Behaviour, General Identity Theft Beliefs

The first section (6.1) deals primarily with data screening and includes descriptive statistics, convergent and divergent reliability, and normality. The next section (6.2) analyzes TPB using only the 'direct measures' (attitudes, subjective norm, perceived behavioural control, behavioural intention, and behaviour constructs) but without the beliefs of TPB, using the complete sample of 356 (see Table 8 with reference to Table 5). Note that the land registry analysis is special and includes only the 222 respondents that indicated that they owned their home. The final section of Chapter 6 (6.3) addresses the three main components of TPB (see Figure 3) using the full sample but only the general beliefs about identity theft and fraud. Each sub-section deals with one of the three components; attitudes(6.3.1), subjective norm (6.3.2) and perceived behavioural control (PBC) (6.3.3).

Table 8 Observations in Section 6.3 (TPB Analysis without Beliefs)

	Physical Security (n=356)		Monitor Accounts (n=356)		Credit Report (n=356)		Land Registry (n=222)		Password Security (n=356)		Risky Click Link (n=356)		Risky Phone Info (n=356)		Risky Use Remember (n=356)	
Sample	*B	*O	*B	*O	*B	*O	*B	*O	*B	*O	*B	*O	*B	*O	*B	*O
Physical Security		✓		✓		✓		✓		✓		✓		✓		✓
Monitoring Accounts		✓		✓		✓		✓		✓		✓		✓		✓
Monitoring Agencies		✓		✓		✓		✓		✓		✓		✓		✓
Password Security		✓		✓		✓		✓		✓		✓		✓		✓
Risky Behaviours		✓		✓		✓		✓		✓		✓		✓		✓

*B-Behaviour-specific beliefs: Behavioural and Control
*O - Other - Attitudes, Subjective Norm, Perceived Behavioural Control, Behavioural Intention, Behaviour, General Identity Theft Beliefs

Chapter 7 presents the complete TPB model but with the reduced random sub-sample for each of the behavioural components. There is a sub-section for each of the eight analysis groups (see Table 9).

Again, the land registry includes only respondents that indicated that they owned their home. These eight sections are followed by a summary discussion of the TPB results (7.9), results and discussion of the PMT models for all analysis groups (7.10) and a comparison of the TPB and PMT models (7.11). Chapter 8 is devoted to the results and analysis of the qualitative input and includes input from 408 respondents. Chapter 9 examines consumer views on credit card fraud versus other identity fraud.

Table 9 - Observations in Chapter 7 (Complete TPB and PMT Models)

	Physical Security (n=67)		Monitor Accounts (n=66)		Credit Report (n=80)		Land Registry (n=49)		Password Security (n=67)		Risky Click Link (n=78)		Risky Phone Info (n=78)		Risky Use Remember (n=78)	
Sample	*B	*O	*B	*O	*B	*O	*B	*O	*B	*O	*B	*O	*B	*O	*B	*O
Physical Security	✓	✓														
Monitoring Accounts			✓	✓												
Monitoring Agencies					✓	✓	✓	✓								
Password Security									✓	✓						
Risky Behaviours											✓	✓	✓	✓	✓	✓

*B-Behaviour-specific beliefs: Behavioural and Control
*O - Other - Attitudes, Subjective Norms, Perceived Behavioural Control, Behavioural Intention, Behaviour, General Identity Theft Beliefs

4.2.4 Phase 2 Survey Instrument Implementation

The Phase 2 survey was approved by the McMaster University Research Ethics Board on December 17, 2012 (Protocol Number: 2012-181). The instrument was administered on the Internet using McMaster University's Lime Survey facility, which guarantees anonymity. The sample was provided by a commercial survey company from one of its standing panels. The company was asked to provide a sample representative of the Canadian population. They were to select members of their panel that were 18 years of age or older and had at least one bank account and one credit card. These characteristics were verified in the initial section of the survey and the session was terminated if the characteristics were not met. French translation was provided by the survey company and incorporated into Lime Survey. Initial language choice was based on the profile maintained by the survey company but could be changed by the respondent at any time. The 'soft launch' with approximately 40 respondents started on Friday, 22 March 2013. After the results were examined to detect problems, the 'full launch' was started on Tuesday, 26 March 2013 and completed on Tuesday, 2 April 2013. The preamble to the survey stated that the time for completion would be about 30 minutes. The average time, excluding cases where the survey was completed in more than one session, was 31.53 minutes. There were 446 completed surveys. As well as their responses to quantitative questions, 408 respondents also provided replies to qualitative questions (see Appendix D, General Questions 10).

Chapter 5. Phase 1 Exploratory Questionnaire Results and Discussion

The Phase 1 exploratory questionnaire was designed primarily as a qualitative instrument to elicit salient beliefs about identity theft and fraud. The exploratory questionnaire is shown in Appendix A.

5.1 Phase 1 Exploratory Questionnaire Results

Following approval by the McMaster Research Ethics Board (Protocol Number: 2012 -17), the exploratory questionnaire was administered using McMaster University's Lime Survey facility in a manner that guaranteed anonymity. An e-mail inviting participation was sent to a demographically diverse convenience sample. Of the 53 invitations, 29 complete (55% response rate) and 2 partial responses (4% response rate) were received. Since the objective of the Phase 1 questionnaire was to elicit salient beliefs, partial responses were included. Qualitative data were analyzed using the techniques and procedures of Strauss and Corbin (1998), using two rounds of coding with the assistance of MaxQDA software. The first round (open coding) generated new codes as new issues were encountered. A second coder independently coded the qualitative data using the codes defined in the first round. The second round rationalized the codes created in the first round. In all, 1016 comments were coded. The frequency of each code and inter-rater reliability measures are shown in Appendix B and a summary is shown in Table 10. The number of codes kept in the Phase 2 survey is shown in the table and the criteria for selection are discussed in sub-section 4.2.1. The four inter-rater reliability measures were all 0.75,[11] which is considered as 'substantial' (Landis and Koch, 1977) or 'excellent' (Fleiss, 1981). The beliefs elicited were used to construct the Phase 2 survey instrument.

[11] The reliability measures discount the percentage agreement by the estimated agreement that might be obtained in the case of random selection. The different agreement measures are due to differing estimates of random agreement. When there are a large number of possible codes, the chances of random agreement are reduced and the differences in the measures become small.

Table 10 - Summary of Preliminary Qualitative Study

Topic	Keep[12]			
	No		Yes	
	Codes	Freq	Codes	Freq
General Outcome	1	3	9	115
General Subjective Norm	6	37	12	196
General Control	16	75	4	57
Physical Security Outcome	1	1	3	22
Physical Security Control	1	8	5	59
Password Outcome	1	1	5	27
Password Control	3	6	6	74
Credit Report Outcome	0	0	3	29
Credit Report Control	0	0	5	27
Monitor Accounts Outcome	0	0	2	26
Monitor Accounts Control	2	2	6	26
Remember Password Outcome	1	1	3	45
Remember Password Control	0	0	4	14
Phone Info Outcome	0	0	6	37
Phone Info Control	1	3	3	12
Click Link Outcome	0	0	5	41
Click Link Control	0	0	2	12
Land Registry Outcome	0	0	5	27
Land Registry Control	0	0	3	19
Total	33	137	91	865

Although the sample size was statistically small, the few quantitative items in the Phase 1 study provided some interesting results (charts of the quantitative item results are shown in Appendix C). Almost 60% of respondents rated their chances of their personal identity information being stolen, if they did nothing to prevent it, as 'quite likely' or 'extremely likely'. Only 14% rated it

[12] 'Keep' indicates whether the code was used in the final quantiative instrument. The criteria for inclusion are discussed in section 4.2.

as at all unlikely. There was almost unanimous agreement that the consequences of identity theft are serious; 27 (93%) rated the consequences as 'quite serious' or 'extremely serious'. 20 (69%) of the respondents rated the difficulty of protecting personal identity information as 'slightly difficult' or 'quite difficult'. Slightly more than half (16) were 'slightly satisfied' or 'quite satisfied' with their current precautions against identity theft. Feelings about their ability to detect identity fraud were quite ambivalent, with 20 (69%) rating themselves as either 'slightly unsure' or 'slightly confident'. The frequency chart for ability to detect identity fraud is completely symmetrical around the ‘neither unsure nor confident’ rating.

5.2 Phase 1 Exploratory Questionnaire Discussion

Respondents took identity theft as a serious problem, with most rating the consequences as very serious and the chances of being a victim, in the absence of precautions, as especially likely. They rated the precautions required to prevent identity theft as moderately difficult and were generally satisfied with their current precautions. They were, on average, undecided about their ability to detect identity theft after it occurs. As for their experience with identity theft, only 41% (12 respondents) had never been the victim of fraudulent credit card usage and 24 % had been victims within the last year. Other identity theft was less frequent, with 10% (3 respondents) experiencing it.

Chapter 6. Phase 2 Full Sample Results and Discussion

The full sample of responses had direct measures for attitudes, subjective norm, perceived behavioural control, intent and reported behaviour. It also had general behavioural beliefs, normative beliefs and general control beliefs. This allowed for analysis of TPB excluding beliefs (Hypotheses HT3, H5, HT8 and HT9) and the analysis of the general beliefs on attitudes, subjective norm and perceived behavioural control (HT2, HT4 and HT7). The following sections deal with TPB without beliefs (6.2), general behavioural beliefs (6.3), normative beliefs (6.4), and general control beliefs (6.5), all using the full sample. The first section (6.1) deals with data screening results.

6.1 Phase 2 Data Screening

A ‘quality assurance’ question at the end of the ‘general’ questions asked respondents to complete a specific response to indicate that they had read the survey questions carefully (see last item in question 21 of Appendix D, General Questions 9, page 193). Eliminating responses from respondents who appeared not to have read the questions carefully left 361 complete quantitative responses where the respondents had apparently carefully read the questions. Examination of the remaining observations revealed that 5 individuals had selected the same response for all of the 76 direct measure items. To ensure that these were not legitimate, the start and end times for completion of the survey were examined. All of the times were significantly lower than the average time and in one case the respondent had taken only three minutes to complete the entire survey. Given that some of the items were reverse-coded and because of the short time for completion, it was deemed that these respondents had not honestly completed the survey and their responses were excluded from further analysis.

The breakdown of the final accepted observations randomly assigned to the five behaviour-specific question groups is in Table 11, representing a total of 356 valid and complete responses to the quantitative questions.

Table 11 - Random Section Selection

Assignment	Count	Percent
Monitor Agencies	80	22.5
Monitor Accounts	66	18.5
Secure Passwords	65	18.3
Physical Security	67	18.8
Risky Behaviours	78	21.9

The demographics of the respondents are displayed in Appendix E. A comparison of the sample with the characteristics of the overall population is in Appendix F. The sample is relatively representative of the entire population, but with the 26-35 age group over-represented and the over 65 age group under-represented. This may be expected given that the survey was administered over the Internet and older people are less likely to be Internet users than the general population.

6.1.1 Outliers

Both the Mahalanobis and Cook distances were computed to detect outliers. In only one instance did Cook's distance exceed the value of 0.04282 (n=356 and k=1) specified by Kim and Storer (1996) as worthy of investigation. The Mahalanobis distances were more problematic: 30 responses (8.43%) exceeded the 186.76 Chi Square critical value for 131 degrees of freedom at the 0.001 confidence level (see Figure 8). The relatively smooth distribution suggests that the highest values were not outliers. Examination of the observations exceeding the critical value showed that these respondents tended to select the extreme values on the scale instead of the moderate values available. Given that many of the observations that typically would lead to high Mahalanobis distances had already been eliminated through the use of the quality assurance question and the removal of 'same response' submissions, and in light of the smooth distribution, it was decided that all remaining 356 observations should be included for analysis.

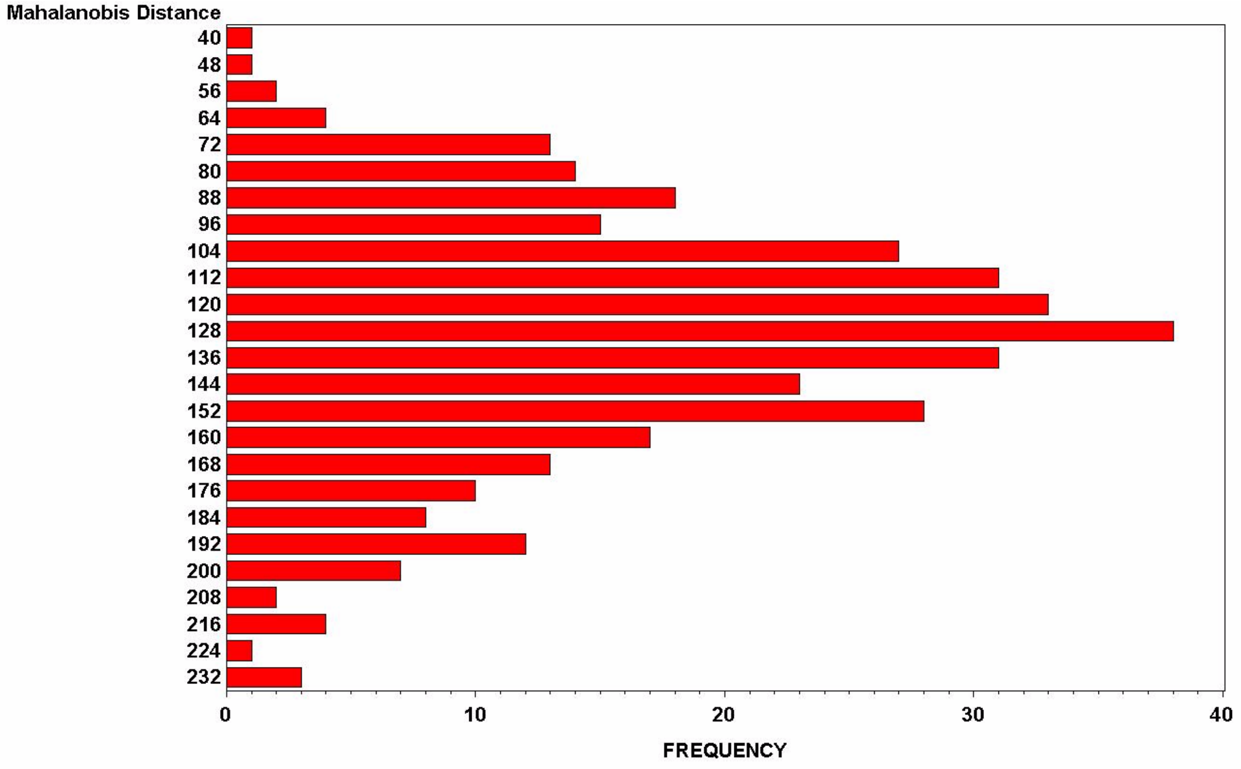


Figure 8 - Mahalanobis Distance Frequency Distribution

6.1.2 Validity

The combined loadings and cross-loadings for all latent variables for the items completed by all respondents are shown in Appendix G. For convergent validity, it is recommended that the criteria be a loading of greater than 0.5 and a p value of less than 0.05 for reflective latent variables (Hair et al., 1987, 2009). Only two items exceeded the 0.05 p value criterion: G62 ("Clicking on a link in an e-mail is up to me") at 0.217 and G71 ("Giving personal information over the phone is up to me") at 0.278. The loading on their respective latent variables was also unacceptable at 0.172 (perceived behavioural control of clicking on a link in an e-mail) and 0.201 (perceived behavioural control of giving personal information over the phone). Both items were dropped from their respective latent variables. Item G06 ("My friends protect their personal information") had an acceptable p value of <0.001 but the loading onto the subjective norm latent variable was only 0.439. Since there were already three other items in the construct, G06 was dropped. Similarly G10 ("Monitoring my bank account and credit cards is interesting") had a p value of <0.001 but a loading of 0.476 and was dropped from the Monitoring Accounts Attitude construct. G53 ("Whether to use 'remember password' is up to me") had an acceptable p value of 0.046 but a marginally low loading of 0.458. Since it was one of only three items in its construct, it was decided to retain this item. While the p value of I03 ("I know many people who have been victims") was <0.001, its loading onto the PMT vulnerability construct was marginal at 0.588. Since there were three other items in the construct, it was decided to drop I03. Doing so raised the Cronbach's alpha from 0.74 to 0.79.

Convergent validity may also be assessed using the Average Variance Extracted (AVE) (see Appendix H). The recommended minimum for reflective variables is 0.5 (Fornell and Larcker, 1981). The only construct that failed this test (after the eliminations suggested above) was Remember Password Perceived Behavioural Control at 0.447. Since the composite reliability was 0.70 and the AVE failed to meet the heuristic by only 0.05, the construct was retained as originally specified. The AVE of all other constructs exceeded 0.5.

Discriminant validity is indicated by low cross-loadings. Cross-loadings where the absolute value was greater than 0.5 are shown in Table 12.

Table 12 - High Value Cross-Loadings

Type	Construct	Item	Description	Cross Loading
Attitude	Click on Link	G72	Give personal info over phone (valuable)	-0.538
	Monitor Accounts	*G71*	*Give personal info over phone up to me*	*0.700*
	Click on Link	G65	Make an effort to click on links	-0.545
Control	Monitor Accounts	G44	Whether I secure documents is up to me	0.611
	Secure Passwords	*G62*	*Click on a link in an e-mail is up to me*	*0.579*
Intent	Click on Link	G72	Give personal info over phone (valuable)	0.541
	Credit Report	*G06*	*Friends protect their personal info*	*0.599*
	Credit Report	G23	Check my credit report (easy)	0.526

G71, G62 and G06 (*italics* in the table) had already been slated for deletion because of poor loading on their intended construct. All of the remaining items with the exception of G44 at least load onto their own component behaviours (G72 and G65 onto 'risky behaviours' and G23 onto 'credit report'). G44 may just be 'noise' . With approximately 2,000 elements in the table, even at a significance level of 0.001 one would expect a few errant values. Furthermore, when behaviour-specific models are analyzed, the high-value cross-loading constructs (with the exception of G65 and G23) appear in different models. No further deletions were made.

6.1.3 Reliability

Reliability was assessed using Cronbach’s alpha and composite reliability, which are shown in Appendix H. The conservative recommendation is that both measures should equal or exceed 0.7 (Fornell and Larcker, 1981; Nunnally, 1978; Nunnally and Bernstein, 1994). A more relaxed criterion is that one of the measures should be equal to or greater than 0.7 (Fornell and Larcker, 1981). All measures exceeded this limit with the exception of Remember Password Perceived Behavioural Control, with a composite reliability of 0.698 and a Cronbach’s alpha of 0.362. It did, however, pass the ‘relaxed’ threshold of 0.6 (Nunnally and Bernstein, 1994).

6.1.4 Normality

One of the requirements of SEM is for the distributions of the variables to be normal. Appendix I provides the descriptive statistics of the items in the survey for all respondents. As indicated by the skewness measure, most distributions were quite skewed. Computing the values of the latent variables from the reflective/formative items resulted in the descriptive statistics in Appendix J. Frequency charts of the latent variables appear in Appendix K. Visual inspection showed that most were highly skewed and monotonically increasing or decreasing. Using Lilliefors modification of the Kolmogorov-Smirnov test for normality to account for unknown means and variances (Lilliefors, 1967) showed that none of the K-S D values for the latent variables exceeded the critical value at the 0.01 significance level, indicating that the sampling distributions for all latent variables were not normal. While in theory departures from normality degrade the performance of SEM analysis, Tabachnick and Fidell (2006) state that "normality of the variables is not always required for analysis" (p79). Hair et al. (2010) contend that departures from normality are negligible when sample sizes are greater than 200. The full sample of 356 observations in this study substantially exceeded this limit. For the smaller randomly selected sub-samples, PLS is robust against departures from normality (Chin and Newstad, 1999; Gefen et al., 2000). Goodhue, Lewis and Thompson (2012) found PLS "remarkably robust against moderate departures from normality" and extremely skewed data resulted in about a 25% drop in power for the sample sizes in this study. Transformations might be considered but with a limited range of possible values (limited because of the 7-point Likert scale and usually only three items or less in a construct), the distribution would still be 'lumpy'. Furthermore there are problems such as interpretability with transformations (Pearson and Please, 1975). It was decided to use the data without transformation and live with any reduction in power.

6.1.5 Random Selection

The assignment to sub-sample groups was accomplished using a random number selection in the survey software. To ensure that the groups were, in fact, homogeneous, Multiple Analysis of Variance (MANOVA) was performed using demographic variables (age, language, gender, home ownership, number of bank accounts and number of credit cards). Box's test of equality of covariance matrices (Box, 1949) yielded a statistically insignificant value of 0.429, indicating that the hypothesis of equal covariance matrices across all groups could not be rejected. Tests of between-subject effects showed that there were no significant differences at the 0.05 level between groups for any of the demographic variables (see Appendix T). The only demographic variable with a difference that was close to significant at the 0.05 level was the number of credit cards, at 0.070. Tukey's HSD post hoc tests of comparisons between groups for the number of credit cards (also in Appendix T) showed no statistically significant differences at the 0.05 level. The selection was therefore deemed appropriately random.

6.1.6 Principal Components Analysis

Since the research was predicated on the five principal components identified by Gilbert and Archer (2012), it was appropriate to ensure that the components had remained stable. The Kaiser-Meyer-Olkin Measure of Sampling Adequacy was 0.699, which by the slimmest of margins failed to meet the minimum heuristic level of 0.70 (Kaiser, 1970, 1974), but Bartlett's test of sphericity was significant at the 0.001 level. Furthermore, the communalities (shown in Table 13) had a minimum value of 0.553, indicating a substantial level of contribution for all items and that no items should be deleted.

Table 13 - Communalities of Principal Components

H01	Monitor credit card accounts	0.820
H02	Monitor bank account balances	0.839
H03	Request a copy of my credit report	0.748
H04	Check land registry office records	0.701
H05	Use hard-to-break passwords	0.603
H06	Have different passwords	0.619
H07	Use a locked mailbox for incoming mail	0.704
H08	Shred financial or important documents	0.553
H09	Keep financial info in secure place	0.601
H10	Use "remember my password"	0.558
H11	Give personal information over the phone	0.616
H12	Click on link in e-mail	0.663

To maintain consistency with the research plan, the analysis was done specifying 5 factors. The pattern matrix is shown in Table 14 (see Appendix M for eigenvalues and scree plot).

The factors are not radically different from those identified by Gilbert and Archer (2012)[13]. Factor 2 matches the 'checking agencies' factor of Gilbert and Archer and factor 3 matches the 'monitoring accounts' factor. The 'passwords' factor and 'physical security' factors have basically loaded onto factor 1, with the exception of the 'use a locked mailbox for incoming mail' item. It is possible that the use of a locked mailbox is biased by the type of accommodation and where respondents reside. All apartments, whether rented or condominiums, have locked mailboxes.

[13] It should be noted that Gilbert and Archer had a sample size of more than 3,000. Their principal components analysis should be considerably more relilable.

Table 14 - 5 Factor Pattern Matrix with Oblimin Oblique Rotation

Behaviour		Factor				
		1	2	3	4	5
H06	Have different passwords	**0.763**	0.003	0.130	0.207	-0.049
H05	Use hard-to-break passwords	**0.715**	0.084	0.162	0.064	-0.178
H08	Shred financial or important documents	**0.671**	-0.066	0.005	-0.157	0.214
H09	Keep financial info in secure place	**0.632**	0.141	-0.102	-0.065	0.337
H03	Request a copy of my credit report	-0.013	**0.872**	0.065	-0.051	-0.048
H04	Check land registry office records	0.005	**0.816**	-0.036	0.059	0.087
H02	Monitor bank account balances	0.049	0.001	**0.894**	-0.130	-0.004
H01	Monitor credit card accounts	0.062	0.035	**0.890**	-0.006	0.014
H12	Click on link in e-mail	0.115	-0.090	-0.010	**0.824**	0.067
H11	Give personal information over the phone	-0.036	0.143	-0.137	**0.735**	-0.095
H07	Use a locked mailbox for incoming mail	0.142	0.072	0.010	-0.052	**0.804**
H10	Use "remember my password"	-0.424	-0.025	0.209	0.297	**0.471**

Bold indicates items that correlate most strongly with their respective factor.

In Canada, suburban residents have been served by community mailboxes for many years which are also locked. In fact, only 33% of addresses get door-to-door delivery (Canada Post, 2013) taking the option of an unlocked mailbox out of the hands of the majority of Canadian consumers. The 'risky behaviours' factor is the same as factor 4 but excludes the 'use "remember my password"' item. The two 'orphaned' items load onto factor 5. The only cross-loading of note is the -.424 loading of “remember my password” onto factor 1, which contains the two password security items (H06 and H05). It appears that those who take passwords seriously are disinclined to use "remember my password". To provide a cleaner analysis, the analysis was conducted again specifying 6 factors. The result is shown in Table 15.

Table 15 - 6 Factor Pattern Matrix with Oblimin Oblique Rotation

Behaviour		Factor					
		1	2	3	4	5	6
H09	Keep financial info in secure place	**0.789**	0.124	-0.131	-0.106	0.119	0.169
H08	Shred financial or important documents	**0.737**	-0.080	-0.008	-0.158	0.090	0.008
H06	Have different passwords	**0.722**	-0.005	0.128	0.208	-0.105	-0.101
H05	Use hard-to-break passwords	**0.558**	0.079	0.183	0.117	-0.090	-0.326
H03	Request a copy of my credit report	0.027	**0.870**	0.058	-0.082	-0.080	0.019
H04	Check Land Registry Office records	-0.028	**0.814**	-0.024	0.074	0.142	-0.058
H02	Monitor bank account balances	-0.022	0.002	**0.912**	-0.094	0.031	0.029
H01	Monitor credit card accounts	0.008	0.035	**0.904**	0.016	0.021	0.086
H12	Click on link in e-mail	-0.031	-0.087	0.018	**0.858**	0.167	-0.016
H11	Give personal information over the phone	-0.017	0.146	-0.150	**0.672**	-0.162	0.169
H07	Use a locked mailbox for incoming mail	0.055	0.062	0.058	0.077	**0.936**	-0.013
H10	Use "remember my password"	0.022	-0.032	0.129	0.103	-0.017	**0.938**

Bold indicates items that correlate most strongly with their respective factor.

All behaviours load onto the same factors as the 5 factor analysis, with the exception of the two 'orphan' behaviours (H07 - Use a locked mailbox for incoming mail and H10 - Use "remember my password"), which loaded onto separate factors. The cross-loading of H10 onto factor 1 decreased to only 0.022. The loading of "remember my password" (H10) onto a different factor than 'risky behaviours' (factor 4) is not a concern, since, as one of the risky behaviours (H10, H11 and H12), it was analyzed separately.

The principal components analysis was conducted using all the responses for the behavioural items. Since the land registry item did not apply if the respondents did not own their home, there was a question as to the validity of their input to this item. To ensure that this was not a problem, the response to item H04 for home non-owners was replaced by imputed values and the analysis was conducted again. The resulting pattern matrix is shown in Appendix N. The same items loaded onto the same factors, so this is not a problem.

6.2 Phase 2 Full Sample TPB without Beliefs

This section is an analysis of the full sample of 356 observations that had direct attitude and perceived behaviours control measures for all studied behaviours. The portions of the TPB included are shown in Figure 9.

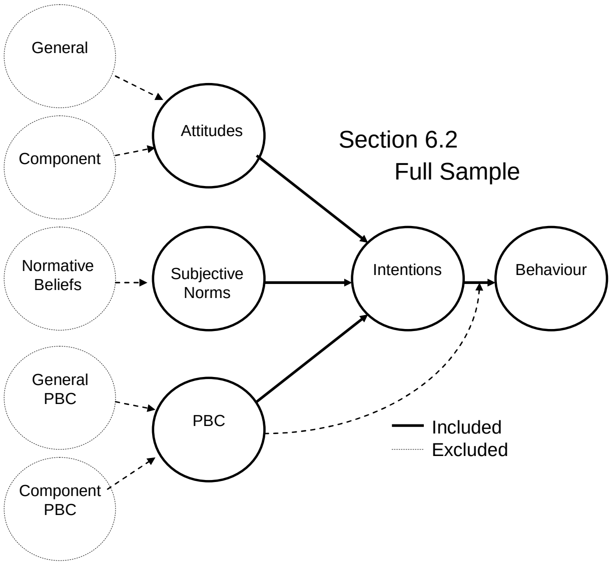


Figure 9 -Parts of TPB Model Included in Section 6.2

The TPB model for the ‘monitoring accounts’ behaviour component is depicted in Figure 10. Attitudes, subjective norm, perceived behavioural control (PBC) and intent variables were modeled as reflective, and component behaviours as formative. Analysis was conducted using PLS with bootstrapping, using 100 resamples. It has been shown that higher numbers of resamples leads to negligible improvements in p values (Effron et al., 2004; Goodhue, Lewis and Thompson, 2012). Bootstrapping was chosen since it tends to produce more reliable p values for larger (more than 100) sample sizes (Nevitt and Hancock, 2001).

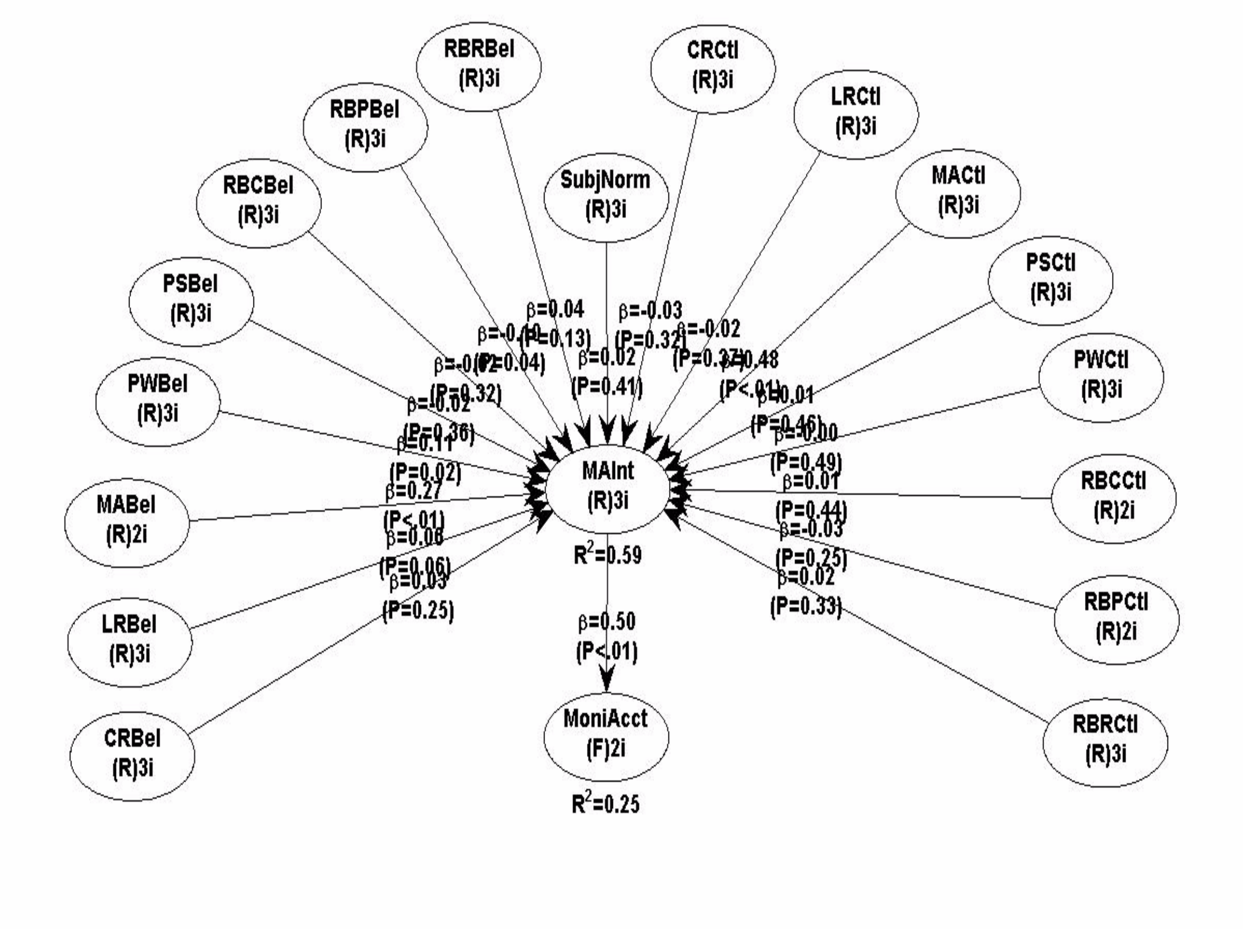


Figure 10 - Monitor Agencies TPB Model without Beliefs

The intent of this analysis is to consider the hypotheses that involve attitude, subjective norm, perceived behavioural control (PBC) and the performance of the behaviour (Hypotheses HT3, HT5, HT8 and HT9), and specifically whether attitudes and PBC for one behavioural analysis group have effects on the intention to perform other behaviours. The descriptions of the constructs in Figure 10 are as follows:

CRBel	Credit Report Attitude
LRBel	Land Registry Attitude
MABel	Monitor Accounts Attitude
PSBel	Physical Security Attitude
PWBel	Secure Password Attitude
RBCBel	Click on Link Attitude
RBPBel	Give Info Over Phone Attitude
RBRBel	Use "Remember Password" Attitude
SubjNorm	Subjective Norm
CRCtl	Credit Report Perceived Behavioural Control
LRCtl	Land Registry Perceived Behavioural Control
MACtl	Monitor Accounts Perceived Behavioural Control
PSCtl	Physical Security Perceived Behavioural Control
PWCtl	Secure Password Perceived Behavioural Control
RBCCtl	Click on Link Perceived Behavioural Control
RBPCtl	Give Info Over Phone Perceived Behavioural Control
RBRCtl	Use "Remember Password" Perceived Behavioural Control
MAInt	Intention to Monitor Accounts
MoniAcct	Monitoring Accounts Behaviour

Similar models were constructed for each of the eight analysis groups:

Credit Report
Land Registry
Monitor Accounts
Physical Security
Password Security
Click on Link in E-mail
Give Personal Information over the Phone
Use "Remember My Password"

In each model, all of the eight attitude constructs, subjective norm and all of the eight PBC constructs were linked to the intention construct for the behaviour group being analyzed. The intention construct was then linked to the self-reported behavioural construct for the behavioural group. Note that only the 222 home owners were included in the land registry model. In the models where there was more than one behaviour in the performance construct (monitor accounts, physical security, and password security), the behaviour variable was modeled as a formative construct of the component behaviours. All other constructs were modeled as reflective.

6.2.1 Phase 2 Full Sample TPB without Beliefs - Results

The model estimates for the path from attitude, subjective norm and perceived behavioural control to intention for all eight models are shown in Table 16. The model estimates for the path from intention to self-reported behaviour are in Table 17. (Note that the WarpPLS software standardizes all variables before analysis.)

Table 16 - Parameter Estimates for TPB Models with No Beliefs - Paths to Intention

	Behaviour Group Intention							
	Credit	Land	Monitor	Physical	Secure	Click	Info Over	Remember
Path Coefficients	Report	Registry	Accounts	Security	Passwords	Link	Phone	Password
Credit Report Attitude	**0.671**	**0.240**	0.033	-0.019	0.029	0.103	0.018	-0.049
Land Registry Attitude	0.083	**0.536**	0.063	0.050	-0.007	-0.046	0.055	-0.026
Monitor Accounts Attitude	0.055	-0.001	**0.271**	0.017	0.067	-0.051	**-0.129**	-0.001
Physical Security Attitude	0.098	0.025	-0.022	**0.554**	0.136	-0.028	0.005	-0.055
Secure Password Attitude	0.032	0.112	0.105	0.080	**0.331**	-0.039	-0.032	0.032
Click on Link Attitude	-0.022	-0.009	-0.025	0.027	0.073	**0.754**	**0.151**	0.063
Give Info Over Phone Attitude	0.009	0.133	-0.100	-0.031	-0.079	-0.017	**0.506**	0.034
Use Remember Password Attitude	-0.034	-0.080	0.044	-0.098	-0.068	0.046	0.005	**0.648**
Subjective Norm	**-0.128**	0.075	0.016	-0.041	0.007	0.030	-0.084	-0.056
Credit Report PBC	**0.187**	-0.062	-0.028	0.129	0.035	-0.048	-0.105	-0.039
Land Registry PBC	-0.018	**0.194**	-0.017	0.015	0.055	-0.029	0.004	0.035
Monitor Accounts PBC	**-0.224**	-0.105	**0.479**	-0.007	0.085	-0.063	-0.052	-0.060
Physical Security PBC	-0.070	-0.088	0.005	0.047	0.003	-0.047	-0.012	0.040
Secure Password PBC	0.067	-0.097	-0.001	0.085	**0.265**	0.060	0.010	-0.015
Click on Link PBC	-0.003	-0.020	0.008	0.053	-0.001	0.034	**-0.159**	**-0.159**
Give Info Over Phone PBC	0.006	-0.093	-0.033	-0.109	-0.084	0.011	**0.193**	-0.008
Use Remember Password PBC	-0.036	0.013	0.021	-0.023	0.050	0.006	-0.035	**0.218**

Table 16 Cont'd

	Behaviour Group Intention							
p Values	Credit Report	Land Registry	Monitor Accounts	Physical Security	Secure Passwords	Click Link	Info Over Phone	Remember Password
Credit Report Attitude	**<0.001**	**<0.001**	0.254	0.371	0.287	0.012	0.337	0.119
Land Registry Attitude	0.020	**<0.001**	0.056	0.173	0.434	0.243	0.080	0.304
Monitor Accounts Attitude	0.095	0.494	**<0.001**	0.357	0.062	0.135	**0.002**	0.491
Physical Security Attitude	0.027	0.316	0.360	**<0.001**	0.011	0.263	0.455	0.134
Secure Password Attitude	0.241	0.036	0.018	0.070	**<0.001**	0.133	0.250	0.258
Click on Link Attitude	0.272	0.443	0.316	0.284	0.063	**<0.001**	**0.002**	0.098
Give Info Over Phone Attitude	0.416	0.023	0.042	0.252	0.042	0.346	**<0.001**	0.213
Use Remember Password Attitude	0.212	0.059	0.133	0.017	0.058	0.109	0.446	**<0.001**
Subjective Norm	**<0.001**	0.079	0.408	0.184	0.442	0.189	0.037	0.098
Credit Report PBC	**<0.001**	0.172	0.322	0.012	0.273	0.158	0.031	0.155
Land Registry PBC	0.319	**<0.001**	0.374	0.376	0.128	0.255	0.466	0.241
Monitor Accounts PBC	**<0.001**	0.058	**<0.001**	0.447	0.053	0.087	0.194	0.101
Physical Security PBC	0.111	0.101	0.463	0.216	0.476	0.186	0.400	0.190
Secure Password PBC	0.116	0.080	0.488	0.127	**<0.001**	0.095	0.405	0.388
Click on Link PBC	0.473	0.373	0.438	0.165	0.496	0.199	**<0.001**	**0.002**
Give Info Over Phone PBC	0.450	0.056	0.250	0.030	0.043	0.402	**<0.001**	0.435
Use Remember Password PBC	0.194	0.421	0.332	0.325	0.140	0.438	0.241	**<0.001**

Effect Sizes	Credit Report	Land Registry	Monitor Accounts	Physical Security	Secure Passwords	Click Link	Info Over Phone	Remember Password
Credit Report Attitude	**0.532**	**0.140**	0.006	0.006	0.007	0.004	0.001	0.006
Land Registry Attitude	0.037	**0.425**	0.008	0.013	0.001	0.003	0.002	0.001
Monitor Accounts Attitude	0.005	0.000	**0.157**	0.006	0.028	0.011	**0.054**	0.000
Physical Security Attitude	0.030	0.008	0.008	**0.409**	0.078	0.005	0.001	0.014
Secure Password Attitude	0.006	0.018	0.043	0.040	**0.223**	0.008	0.010	0.006
Click on Link Attitude	0.001	0.000	0.006	0.004	0.013	**0.610**	**0.068**	0.016
Give Info Over Phone Attitude	0.000	0.012	0.043	0.008	0.029	0.008	**0.370**	0.010
Use Remember Password Attitude	0.001	0.002	0.008	0.027	0.016	0.014	0.001	**0.507**
Subjective Norm	**0.006**	0.013	0.007	0.018	0.003	0.005	0.032	0.016
Credit Report PBC	**0.086**	0.016	0.010	0.052	0.014	0.009	0.030	0.005
Land Registry PBC	0.004	**0.103**	0.003	0.004	0.015	0.003	0.001	0.002
Monitor Accounts PBC	**0.000**	0.005	**0.339**	0.003	0.047	0.020	0.026	0.015
Physical Security PBC	0.009	0.005	0.002	0.022	0.002	0.012	0.005	0.006
Secure Password PBC	0.008	0.004	0.001	0.042	**0.176**	0.013	0.004	0.003
Click on Link PBC	0.000	0.003	0.000	0.005	0.000	0.014	**0.017**	**0.014**
Give Info Over Phone PBC	0.000	0.009	0.003	0.018	0.011	0.003	**0.058**	0.001
Use Remember Password PBC	0.004	0.002	0.002	0.002	0.002	0.001	0.001	**0.102**
R Squared	0.693	0.719	0.587	0.608	0.639	0.682	0.633	0.666

Bold indicates p value significance at 0.01 level.

The model estimates for the path from intention to self-reported behaviour are shown in Table 17.

Table 17 - Parameter Estimates for TPB Models with No Beliefs - Path from Intent to Behaviour

	Self-Reported Behaviour							
	Credit Report	Land Registry	Monitor Accounts	Physical Security	Secure Passwords	Click Link	Info Over Phone	Remember Password
Path Coefficients	**0.585**	**0.360**	**0.502**	**0.497**	**0.552**	**0.551**	**0.476**	**0.647**
p Values	**<0.001**	**<0.001**	**<0.001**	**<0.001**	**<0.001**	**<0.001**	**<0.001**	**<0.001**
Effect Size	**0.342**	**0.130**	**0.252**	**0.247**	**0.304**	**0.304**	**0.227**	**0.419**
R Squared	0.342	0.130	0.252	0.247	0.304	0.304	0.227	0.419

Bold indicates p value significance at 0.01 level.

6.2.2 Phase 2 Full Sample TPB without Beliefs - Discussion

In all cases, attitude had a positive effect on the intention to perform the related behaviour at the .001 significance level, and six of the eight had effect sizes exceeding the 'substantial' influence heuristic of 0.35 (Cohen, 1988 p.413), confirming Hypothesis HT3 ('An individual’s attitudes toward a behaviour component positively affect the intention to perform the component behaviours.')

Subjective norm has a significant path only to credit report intention; however, this looks suspicious, in that the negative path coefficient implies that the more others think one should perform identity theft prevention behaviours, the less one intends to check his credit report. Hypothesis HT5 ('An individual’s subjective norm positively influences the intention to perform identity theft prevention and detection behaviours') was therefore not supported.

Most of the PBCs had a statistically significant path to ‘their’ behaviour, the exceptions being ‘physical security’ PBC and ‘click on link’ PBC. With the exception of 'monitoring accounts', none of the effect sizes for significant paths reached the 0.15 heuristic for 'moderate' influence (Cohen, 1988 p.413). Hypothesis HT8 ('An individual’s perceived behavioural control of a given behavioural component positively affects the intention to perform component behaviours') was generally, although not strongly, supported. In all columns except ‘monitoring accounts’, the PBC construct had less effect on intention than the attitude construct.

The R squared values for the intention constructs ranged from 0.587 to 0.719, indicating that the majority of the variation had been accounted for in all these constructs.

In all cases, intent had an effect on the actual performance of the related behaviour at the .001 significance level, supporting Hypothesis HT9 ('An individual’s intention to perform component behaviours positively affects the actual performance of the component behaviours').

The R squared values for behavioural performance ranged from 0.130 to 0.419, indicating that other factors accounted for the majority of the variation in performance of the behaviours. These values are lower than those typically quoted. Ajzen (2005 p100), for example, notes correlations between 0.69 and 0.96 (R squared 0.48 to 0.92) between intentions and volitional behaviours. In a meta-analysis of 47 studies specifically targeting the relation between intention and performance, Web and Sheeran (2006) noted, however, that medium to large changes in intentions created only small to medium changes in behaviour. They also observed that intention had even less effect when the behaviour could be habitual. Note that two of the lowest R squared values ('monitoring accounts' at 0.252 and 'physical security' at 0.247) may be considered habitual behaviours. Other meta-analyses investigating primarily health-related behaviours and using TPB or PMT models have also found low correlations between intention and behaviour, as shown in Table 18, where average R squared values range from 0.18 to 0.37. Health-related behaviours are analogous to identity theft prevention and fraud detection behaviours in that individuals must make efforts in the short run to reduce the probability of an undesirable consequence in the long run. Another consideration is the frequency distributions of the intention constructs which were highly skewed, with the exception of land registry, which is almost U shaped. This may have contributed to the low R squared values. It looks as though the road to perdition (or in this case identity theft) is indeed paved with good intentions.

Table 18 - Meta-Analysis Studies with Correlation between Intent and Behaviour

Study	Behaviour	k	n	r_+	r_+^2	FSN
Bamberg and Möser (2007)	Pro-environmental Behaviour	15	5654	.52	.27	N/A
Cooke and French (2008)	Attendance at Screening Programmes	19	8148	.42	.18	141
Hagger and Chatzisarantis (2009)	Physical Activity	28	5822	.61*	.37	5312
Hausenblas, Carron and Mack (1997)	Physical Exercise	32	N/A	.47	.22	39
Rhodes and Dickau (2012)	Physical Activity	11	2167	.51	.26	N/A
Rodgers, Conner and Murray (2008)	Health Behaviours	16	2159	.57	.32	N/A
Trafimow et al. (2002)	Health Behaviours	9	1475	.57	.32	94

* Corrected for both sampling and measurement error
k-number of studies, n-total number of data points, r_+-weighted average correlation between intention and behaviour, FSN-Rosenthal’s (1984) Fail-Safe N[14].

Effect sizes of 0.02, 0.15 and 0.35 are said to indicate small, moderate or substantial influence of an exogenous variable on an endogenous variable respectively (Cohen, 1988, p413). All but one of the effect sizes of intent on behaviour considerably exceeded the lower limit of 0.15 for 'moderate' influence and 'remember password' exceeded the lower limit of 0.35 for 'substantial' influence.

Another intent for these models was to discover if the attitudes and PBC of some behaviours have an influence on the intent to perform other behaviours. The principal components analysis by Gilbert and Archer (2012) of the twelve behaviours revealed an almost orthogonal solution, implying that performing the behaviours in one component had little correlation with performing the behaviours in other components. The parameter estimates for the eight analysis groups (physical security, monitoring accounts, getting credit report, checking land registry, password security, using ‘remember my password’, giving personal information over the phone, and clicking on link in e-mail) indicated that the attitudes and PBCs associated with each analysis group also had little impact on the intent to perform behaviours in other groups. The only cases

[14] Rosenthal’s (1984) Fail-Safe N provides an estimate of the number of unpublished studies comparable in size but containing null results that would be required to invalidate the conclusion that a relationship is statistically significant.

where the attitude of one group had a statistically significant path coefficient to another group were as follows:

Table 19 - Attitudes and PBC That Had a Significant Path to 'Foreign' Analysis Groups

Path	Behaviour Intent	Coefficient	p Value	Effect Size
Credit Report Attitude	Land Registry	0.240	<0.001	0.140
Monitor Accounts Attitude	Info Over Phone	-0.129	0.002	0.054
Click on Link Attitude	Info Over Phone	0.151	0.002	0.068
Click on Link PBC	Info Over Phone	-0.159	<0.001	0.017
Click on Link PBC	Remember Password	-0.159	0.002	0.014

In all cases except the second one (Monitor Accounts Attitude/Info Over Phone), the ‘other’ behaviour is one that is in the same component. In the first case, both credit report and land registry are in the same behavioural component. The last three are all in the ‘risky behaviour’ component, with the last two having very small effect sizes. In the one instance when one behavioural attitude had a statistically significant impact on a different group (i.e. the 'monitor accounts' attitude affecting the 'give information over the phone ' behaviour), the effect size was small. The low correlations between behaviour components appear to extend backwards into the attitudes and PBCs that precede them.

6.3 Phase 2 Full Sample TPB with General Identity Theft Beliefs

The next three sub-sections (6.3.1 - 6.3.3) analyze the impact of general identity theft beliefs on the attitudes, subjective norm and perceived behavioural control for each of the eight analysis groups. Figure 11 shows the parts of the TPB model that are included in each sub-section.

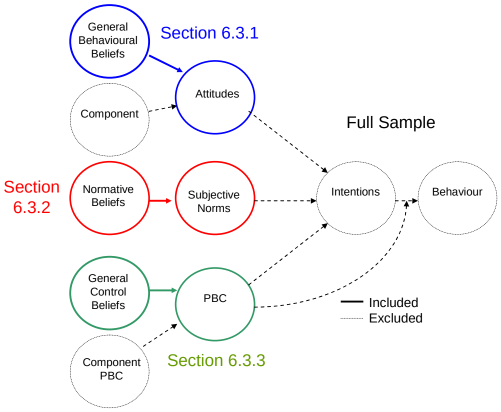


Figure 11 - Parts of TPB Model Included in Sub-sections 6.3.1 - 6.3.3

6.3.1 Phase 2 Full Sample TPB General Behavioural Beliefs

A model for each of the eight behavioural groupings was constructed to examine Hypothesis HT2 ('An individual’s beliefs about identity theft in general influence attitudes toward all behavioural components'); for an example, see Figure 12. For each of the eight analysis groups, the attitude construct was the endogenous variable for the nine general identity theft behavioural beliefs.

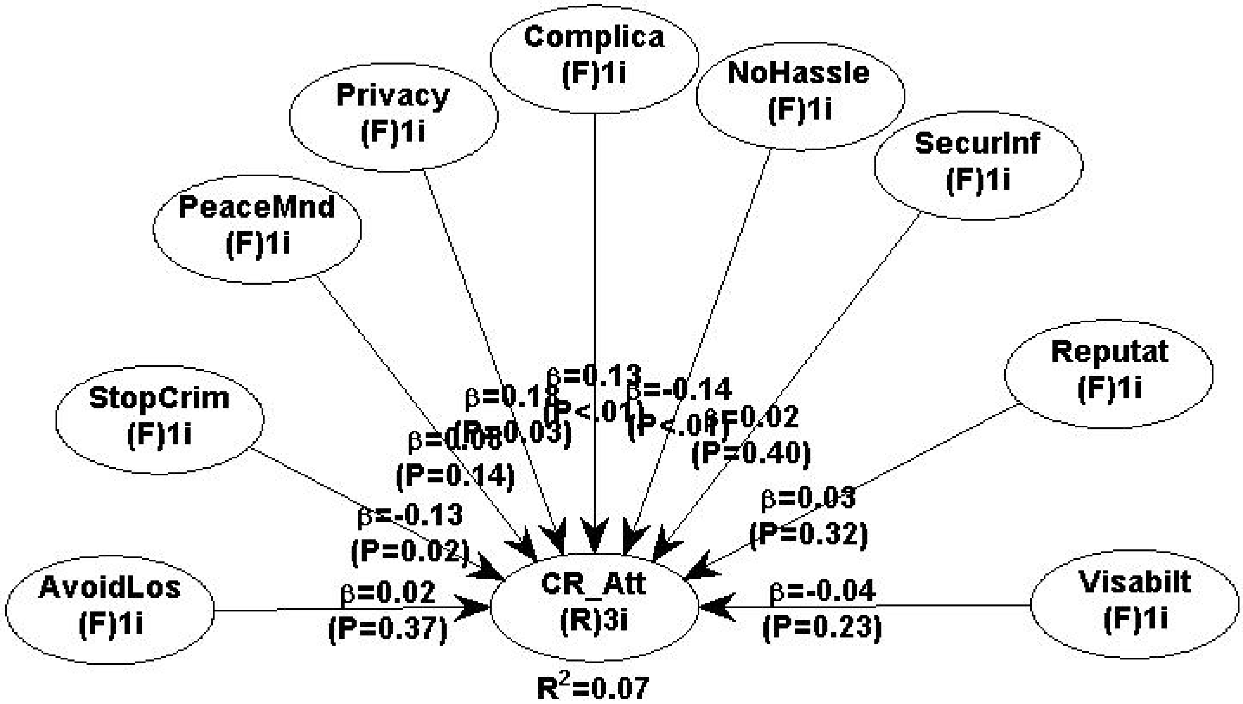


Figure 12 - Behavioural Belief Model for ‘Checking Credit Report’ Attitude

6.3.1.1 Phase 2 Full Sample TPB General Behavioural Beliefs - Results

Parameter estimates for all eight models are shown in Table 21. R Squared values are shown in Table 20:

Table 20 - General Behavioural Beliefs Models - Attitude R Squared Values

	Credit	Land	Monitor	Physical	Password	Click	Info over	Remembr
	Report	Registry	Accounts	Security	Security	Link	Phone	Password
R Squared	0.066	0.105	0.173	0.229	0.176	0.094	0.116	0.021

Table 21 - Model Estimates for General Behavioural Beliefs Affecting Attitudes

Path Coefficients		Credit	Land	Monitor	Physical	Password	Click	Info over	Remember
Variable	Description	Report	Registry	Accounts	Security	Security	Link	Phone	Password
AvoidLos	Avoiding financial loss	0.023	0.016	0.128	0.090	0.049	0.070	-0.009	-0.110
StopCrim	Stopping criminal activity	-0.126	-0.162	-0.050	-0.008	0.042	-0.102	0.002	0.075
PeaceMnd	Having peace of mind	0.081	0.120	0.121	0.100	0.044	-0.099	-0.072	0.034
Privacy	Protecting my privacy	0.181	0.213	**0.287**	**0.273**	0.187	0.022	-0.086	0.016
Complica	Complicating transactions	**0.129**	-0.026	0.070	0.063	0.075	0.111	**0.122**	-0.012
NoHassle	Avoiding the hassle of dealing with fraud	**-0.145**	**-0.177**	0.053	-0.020	-0.054	**0.183**	-0.002	0.038
SecurInf	Securing my personal information	0.023	0.060	-0.024	0.077	0.158	-0.101	-0.108	-0.130
Reputat	Preventing the loss of my reputation	0.028	0.011	**0.106**	-0.009	-0.017	0.111	0.112	0.024
Visabilt	Reducing my online visibility	-0.040	0.089	-0.032	0.097	0.077	-0.090	-0.114	-0.021

P Values		Credit	Land	Monitor	Physical	Password	Click	Info over	Remember
Variable	Description	Report	Registry	Accounts	Security	Security	Link	Phone	Password
AvoidLos	Avoiding financial loss	0.367	0.417	0.059	0.012	0.130	0.117	0.444	0.064
StopCrim	Stopping criminal activity	0.022	0.027	0.250	0.453	0.215	0.066	0.490	0.139
PeaceMnd	Having peace of mind	0.136	0.109	0.049	0.106	0.257	0.071	0.190	0.320
Privacy	Protecting my privacy	0.028	0.027	**<0.001**	**<0.001**	0.020	0.403	0.197	0.433
Complica	Complicating transactions	**0.007**	0.350	0.068	0.077	0.049	0.014	**0.010**	0.409
NoHassle	Avoiding the hassle of dealing with fraud	**0.002**	**0.002**	0.237	0.327	0.054	**<0.001**	0.481	0.287
SecurInf	Securing my personal information	0.399	0.280	0.379	0.166	0.045	0.110	0.075	0.073
Reputat	Preventing the loss of my reputation	0.315	0.440	**0.008**	0.430	0.360	0.027	0.029	0.323
Visabilt	Reducing my online visibility	0.232	0.079	0.212	0.025	0.051	0.062	0.011	0.342

Effect Size		Credit	Land	Monitor	Physical	Password	Click	Info over	Remember
Variable	Description	Report	Registry	Accounts	Security	Security	Link	Phone	Password
AvoidLos	Avoiding financial loss	0.001	0.002	0.032	0.023	0.009	0.003	0.001	0.010
StopCrim	Stopping criminal activity	0.001	0.011	0.010	0.002	0.011	0.015	0.000	0.000
PeaceMnd	Having peace of mind	0.009	0.024	0.040	0.038	0.014	0.015	0.017	0.001
Privacy	Protecting my privacy	0.026	0.053	**0.104**	**0.121**	0.070	0.003	0.023	0.001
Complica	Complicating transactions	**0.013**	0.002	0.003	0.002	0.004	0.014	**0.016**	0.000
NoHassle	Avoiding the hassle of dealing with fraud	**0.014**	**0.013**	0.008	0.002	0.004	**0.020**	0.000	0.000
SecurInf	Securing my personal information	0.002	0.012	0.007	0.029	0.057	0.014	0.028	0.012
Reputat	Preventing the loss of my reputation	0.000	0.000	**0.008**	0.000	0.000	0.011	0.012	0.001
Visabilt	Reducing my online visibility	0.000	0.010	0.003	0.022	0.015	0.009	0.018	0.001

Bold indicates significance at the .01 level

6.3.1.2 Phase 2 Full Sample TPB General Behavioural Beliefs - Discussion

There is some support for HT2 for ‘protecting my privacy’, ‘complicating transactions’, ‘avoiding the hassle of dealing with fraud’ and ‘preventing the loss of my reputation’ at the 0.01 level for at least one of the analysis groups. The 0.01 level was chosen because of the relatively large sample (356 for most behaviours and 222 for land registry), which tends to make even small effect sizes significant. Curiously, the signs on the path coefficients for ‘avoiding the hassle of dealing with fraud’ are the opposite of those to be expected. Why, for example, would one have a more positive attitude toward a behaviour if it increased the likelihood of the hassle of dealing with identity fraud? This may be a case where the majority of the respondents misinterpreted the question. Unexpectedly, ‘avoiding financial loss’, ‘stopping criminal activity’ and ‘having peace of mind’ did not register at the 0.01 level of significance on any behavioural component despite being mentioned frequently in the Phase 1 survey. ‘Securing my personal information’ and ‘reducing my online visibility’ did not figure significantly either. The values of R squared vary from a low of 0.021 to a maximum of 0.229, implying that much of the variation in attitude is unexplained by general beliefs. The effect sizes tell a similar story. None reached the 0.15 level that is considered moderate influence and only 3 exceeded the lower limit of 0.02, which is considered a small influence (Cohen, 1988, p.413). The low R squared values and the weak effect sizes suggest that the support for HT2 is inconclusive. Part of the Theory of Planned Behaviour (Ajzen, 2005) and its predecessor Theory of Reasoned Action (Ajzen and Fishbein, 1980) is that behaviours should be defined in action, target, context and time. It appears that behavioural beliefs about identity theft in general do not figure prominently in explaining attitudes toward specific behaviours.

6.3.2 Phase 2 Full Sample TPB Subjective Norm

A model was constructed to test Hypothesis HT4 ('An individual’s normative beliefs about identity theft positively affect the individual’s subjective norm'). The model is shown in Appendix O. The beliefs were constructed using the TPB methodology of multiplying the strength of the belief that the referent favours the individual performing the behaviour and the inclination of the individual to comply with the wishes of the referent.

6.3.2.1 Phase 2 Full Sample TPB Subjective Norm Results

Removing the non-significant beliefs reduces the model to Figure 13, with the corresponding parameter estimates in Table 22.

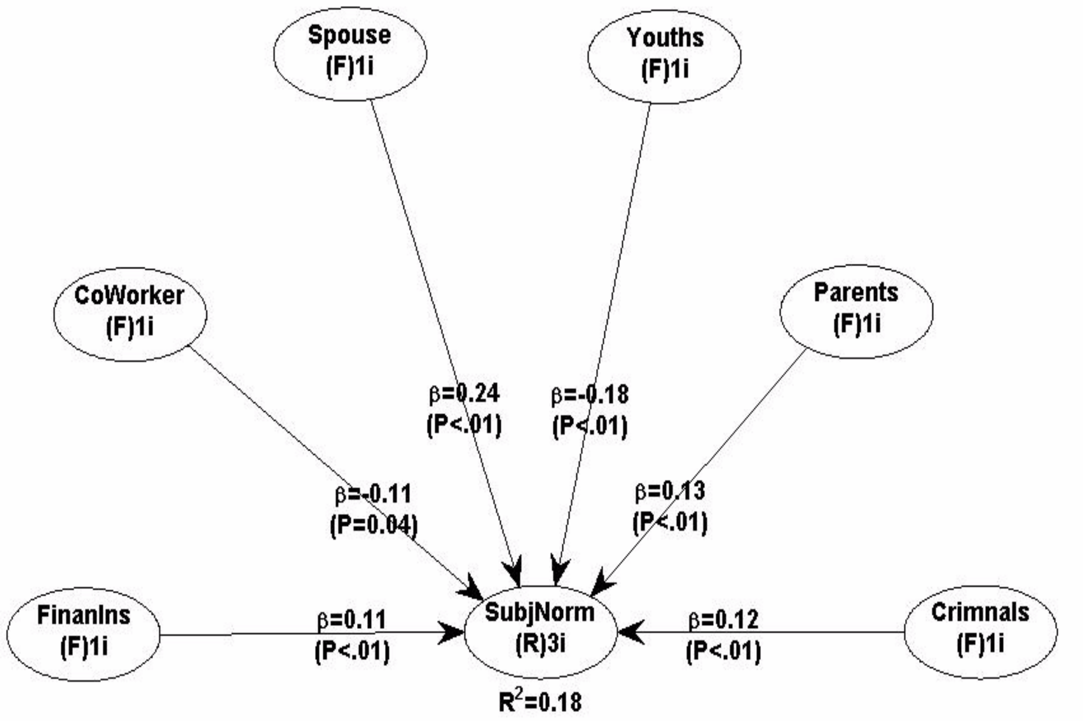


Figure 13 - Normative Belief Model

Table 22 - Normative Belief Model - Significant Paths Only

Variable	Description	Path Coefficient	p Value	Effect Size
FinanIns	Financial Institutions	0.111	0.010	0.015
CoWorker	Co-Workers	-0.105	0.039	0.011
Spouse	Spouse	0.243	<0.001	0.076
Youths	Young people	-0.180	0.001	0.032
Parents	Your parents	0.125	0.010	0.028
Criminals	Criminals	0.115	0.007	0.014
R Squared Value		0.176		

6.3.2.2 Phase 2 Full Sample TPB Subjective Norm Discussion

The scale was a semantic differential balanced around zero (i.e., the scale was -4 to +4). That is how by multiplying the belief that criminals do not want individuals to take identity theft protection measures (-4) and the disinclination of individuals to comply with criminals wishes (-4) can lead to a positive effect on subjective norm. At least some of the normative beliefs affected the subjective norm at significance levels of 0.05 or less. The R squared was only 0.18, so the beliefs failed to explain much of the variance in subjective norm. Only three of the effect sizes exceeded the lower limit of 0.02 and none reached the 0.15 level considered a moderate influence (Cohen, 1988, p.413). The support for HT4 ('An individual's normative beliefs about identity theft positively affect the individual's subjective norm') is very weak. As noted earlier, subjective norm had a minimal effect on intention, so normative beliefs do little to explain behaviour.

6.3.3 Phase 2 Full Sample TPB General Control Beliefs

A model for each of the component behaviours was constructed to examine Hypothesis HT7 ('An individual's control beliefs about identity theft in general influence perceived behavioural control toward all behavioural components'). For each of the eight behavioural groupings, a model with all four general control beliefs was directed to the PBC construct for the group; see Figure 14 for an example. Model parameter estimates are in Table 23.

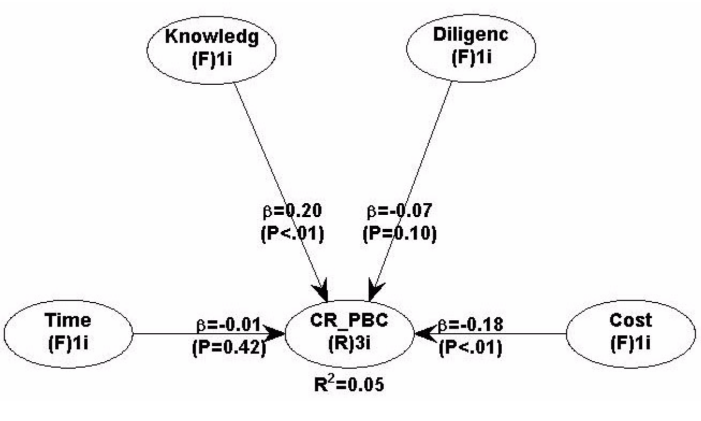


Figure 14 - Control Belief Model for 'Checking Credit Report' Behaviour

Table 23 - Model Estimates for General Control Beliefs Affecting Perceived Behavioural Control

Path Coefficients		Credit	Land	Monitor	Physical	Password	Click	Info over	Remembr
Variable	Description	Report	Registry	Accounts	Security	Security	Link	Phone	Password
Time	Takes a lot of time	-0.011	-0.031	0.067	-0.027	-0.011	-0.035	-0.016	-0.004
Knowledg	Requires a lot of knowledge	**0.195**	**0.238**	**0.161**	**0.299**	**0.255**	-0.008	-0.014	0.093
Diligenc	Requires diligence	-0.069	-0.051	-0.087	**-0.152**	**-0.226**	**0.150**	0.089	0.008
Cost	Costs a lot	**-0.176**	**-0.174**	**-0.178**	**-0.134**	**-0.195**	-0.136	-0.079	-0.144

P Values		Credit	Land	Monitor	Physical	Password	Click	Info over	Remembr
Variable	Description	Report	Registry	Accounts	Security	Security	Link	Phone	Password
Time	Takes a lot of time	0.421	0.316	0.110	0.324	0.432	0.292	0.397	0.473
Knowledg	Requires a lot of knowledge	**<0.001**	**<0.001**	**0.001**	**<0.001**	**<0.001**	0.443	0.398	0.098
Diligenc	Requires diligence	0.097	0.223	0.032	**0.001**	**<0.001**	**0.010**	0.065	0.449
Cost	Costs a lot	**<0.001**	**0.003**	**0.001**	**0.005**	**<0.001**	0.015	0.099	0.015

Effect Size		Credit	Land	Monitor	Physical	Password	Click	Info over	Remembr
Variable	Description	Report	Registry	Accounts	Security	Security	Link	Phone	Password
Time	Takes a lot of time	0.000	0.000	0.004	0.001	0.000	0.002	0.000	0.000
Knowledg	Requires a lot of knowledge	**0.026**	**0.042**	**0.020**	**0.063**	**0.036**	0.000	0.000	0.006
Diligenc	Requires diligence	0.003	0.001	0.005	**0.014**	**0.042**	**0.018**	0.006	0.000
Cost	Costs a lot	**0.026**	**0.026**	**0.024**	**0.014**	**0.035**	0.017	0.006	0.018

Bold indicates significance at the .01 level.

6.3.3.1 Phase 2 Full Sample TPB General Control Beliefs - Results

Model parameter estimates are in Table 23.The R squared values are as follows:

	Credit Report	Land Registry	Monitor Accounts	Physical Security	Password Security	Click Link	Info over Phone	Remembr Password
R Squared	0.054	0.068	0.053	0.090	0.112	0.037	0.013	0.023

6.3.3.2 Phase 2 Full Sample TPB General Control Beliefs - Discussion

Three of the four general control beliefs had a significant path coefficient at the 0.001 level for at least one of the behaviours. ‘Requires a lot of knowledge’ was significant at that level for all of the behaviours except the ‘risky’ behaviours. Indeed, there was almost no support for general control beliefs having an effect on any of the ‘risky’ behaviours. ‘Risky’ behaviours are ‘shortcuts’ designed to make experiences easy and convenient, and as such do not present large control issues, which is evident in the parameter estimates. Surprisingly, ‘takes a lot of time’ did not have any significant path coefficients even at the 0.05 level, even though it was the most frequently mentioned control issue in the Phase 1 survey. While the p values provide support for HT7, the R squared values tell a different story. Excluding the ‘risky’ behaviours, they ranged from 0.053 to 0.112, leaving much of the variance unexplained. The reason for the discrepancy lies in the effect sizes. Three of the statistically significant control beliefs were lower than the heuristic of 0.02 for 'small' influence. None of the control beliefs exceeded the heuristic of 0.15 for 'moderate' influence. While there were statistically significant influences of general control beliefs on perceived behavioural control of specific behaviours, the effects were small, so support for HT7 was unconvincing. Again, as in the connection of behavioural beliefs to attitudes, general control beliefs appeared to have no great explanatory power for the perceived behavioural control of specific behaviours.

Chapter 7. Phase 2 Sub-Samples Results and Discussion

Chapter 7 deals with the results and analysis of the full TPB model, including both general and behaviour-specific beliefs, using data from the sub-samples tailored to each behavioural component, as shown in Figure 15.

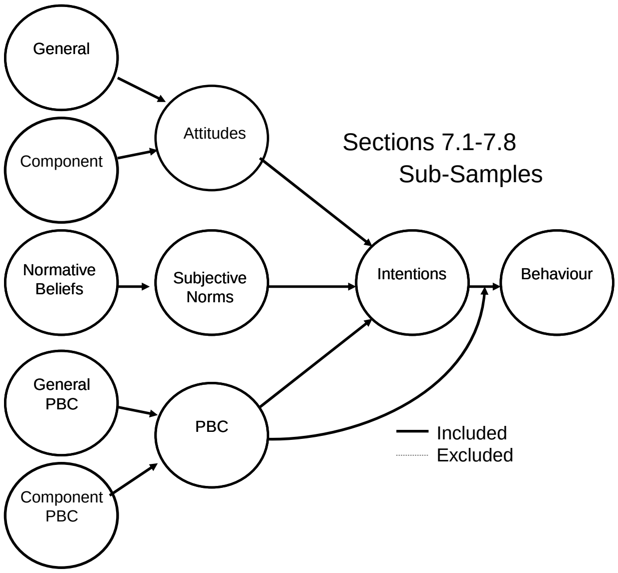


Figure 15 - Parts of the TPB Model Included in Sections 7.1 - 7.8

All models were constructed in WarpPLS using jackknife resampling[15] and PLS Regression. Jackknifing was chosen since it tends to produce more stable path coefficients and p values on small (less than 100) samples (Chiquoine and Hjalmarsson, 2009). PLS Regression (linear) was chosen because it fitted best with TPB, which traditionally has used linear regression and does not propose non-linear relationships. Furthermore, examination of the results using Warp2 Regression (U-curve) and Warp3 Regression (S-curve) on some models did not materially change the results.

All behavioural beliefs were constructed using the TPB method of multiplying the strength of the belief that the outcome would occur by the value of that outcome to the individual. All control beliefs were constructed by multiplying the strength of the belief that the factor would occur by

[15] Note that WarpPLS automatically sets the number of resamples to the sample size for jackknifing.

the perceived power of the factor to impede or facilitate the performance of the behaviour. Full models that include all the general and behavioural specific beliefs and the associated estimates are in Appendix P.

7.1 Phase 2 Sub-sample Credit Report TPB

This section documents the results and discusses the sub-sample (n=80) asked the questions specific to the 'monitoring agencies' component. These questions allowed analysis of the full credit report TPB model for the sub-sample.

7.1.1 Phase 2 Sub-sample Credit Report TPB - Results

Results with the complete TPB model are shown in Appendix P. Keeping only the paths and associated beliefs that have significant p values, the model shown in Figure 16 emerges. The path coefficients and associated p values are in Table 24.

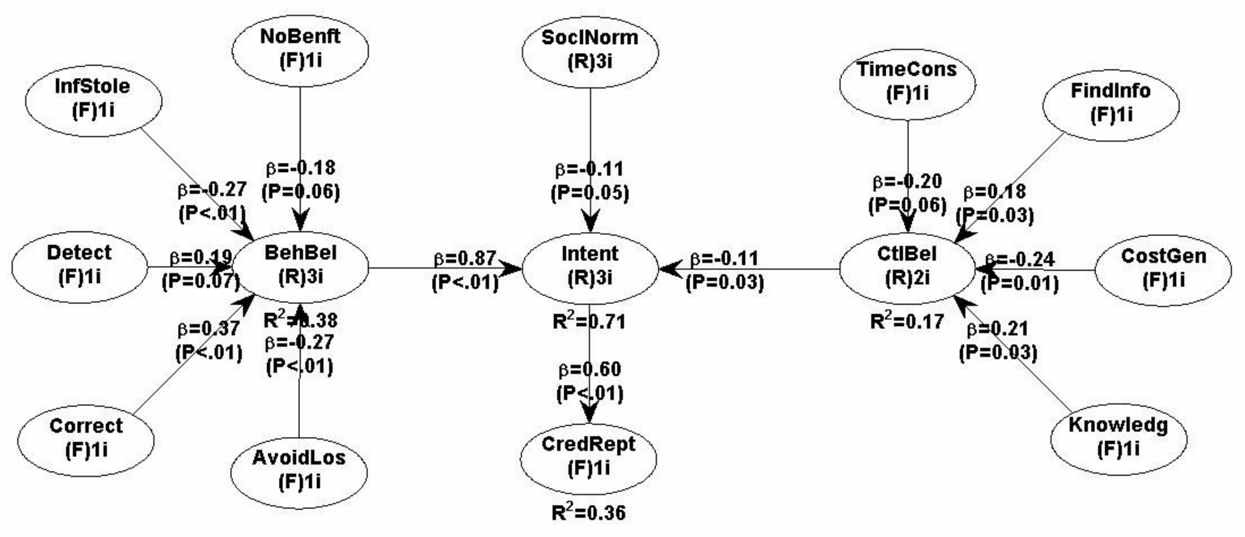


Figure 16 - TPB Model for CredRep ('I request a copy of my credit report at least once a year')

Table 24 - Parameter Estimates for CredRep Model

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to check credit report	0.601			
BehBel	Attitude towards getting credit report		0.874		
CtlBel	PBC towards getting my credit report		-0.109		
SoclNorm	Subjective norm		-0.113		
AvoidLos	Avoiding financial loss (g)			-0.269	
Correct	Correct mistakes			0.374	
Detect	Detect unauthorized use			0.192	
InfStole	Report will be stolen			-0.275	
NoBenft	Get no benefit			-0.176	
Knowledg	Requires a lot of knowledge (g)				0.209
CostGen	Costs a lot (g)				-0.238
FindInfo	Can easily find out how				0.183
TimeCons	Takes too much time				-0.196

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to check credit report	<0.001			
BehBel	Attitude towards getting credit report		<0.001		
CtlBel	PBC towards getting my credit report		0.027		
SoclNorm	Subjective norm		0.048		
AvoidLos	Avoiding financial loss (g)			0.002	
Correct	Correct mistakes			<0.001	
Detect	Detect unauthorized use			0.072	
InfStole	Report will be stolen			0.002	
NoBenft	Get no benefit			0.061	
Knowledg	Requires a lot of knowledge (g)				0.031
CostGen	Costs a lot (g)				0.011
FindInfo	Can easily find out how				0.032
TimeCons	Takes too much time				0.058

Effect Size

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to check credit report	0.362			
BehBel	Attitude towards getting credit report		0.719		
CtlBel	PBC towards getting my credit report		0.001		
SoclNorm	Subjective norm		0.012		
AvoidLos	Avoiding financial loss (g)			0.007	
Correct	Correct mistakes			0.161	
Detect	Detect unauthorized use			0.070	
InfStole	Report will be stolen			0.064	
NoBenft	Get no benefit			0.076	
Knowledg	Requires a lot of knowledge (g)				0.034
CostGen	Costs a lot (g)				0.063
FindInfo	Can easily find out how				0.034
TimeCons	Takes too much time				0.040

	Behaviour	Intention	Attitude	PBC
R Squared	0.362	0.706	0.379	0.171

7.1.2 Phase 2 Sub-sample Credit Report TPB - Discussion

As noted earlier in the discussion of the full sample, Hypotheses HT3 and HT9 were supported. While the path from PBC to intent (HT8) was statistically significant at the 0.05 level, the sign was the opposite of that expected. Furthermore, the effect size was a minuscule 0.001. HT8 was therefore not supported. In this smaller sample, as in the full sample, subjective norm had a significant effect on intention but the sign was negative. H5 was therefore unsupported. One of the general beliefs, 'avoiding loss', had a significant effect on attitude but the coefficient was negative, which is not in the expected direction. This does not constitute support for Hypothesis HT2 ('An individual’s beliefs about identity theft in general influence attitudes toward all behavioural components'). Four of the five beliefs specific to the credit report behaviour had a significant ($p < 0.05$) or marginally significant ($p =0.061$) effect in the expected direction on attitude. The belief that getting a credit report would allow the detection of identity fraud is significant at the 0.001 level. These findings provide support for Hypothesis HT1 ('An individual’s beliefs specific to a behavioural component positively affects attitudes toward that behavioural component'). Two of the four general control beliefs ('requires a lot of knowledge' and 'costs a lot') had a significant effect on PBC at the 0.05 level, providing support for HT7 ('An individual’s control beliefs about identity theft in general influence perceived behavioural control toward all behavioural components'). Two of the three specific control beliefs ('can find out how to get a credit report' and 'takes too much time') were significant or almost significant at the 0.05 level, which provides some support for HT6 ('An individual’s control beliefs specific to a behavioural component positively affect perceived behavioural control toward that behavioural component'). Hypothesis HT10 ('An individual’s perceived behavioural control of a specific behavioural component moderates the influence of the intention to perform component behaviours on the actual performance of the component behaviours') was unsupported.

The 'orthodox' TPB model has shortcomings, however. The R squared on PBC is only 0.171, which implies that much of its variance is unexplained. Examining correlations between variables made possible improvements evident. Dropping the power of control multiplication of the control belief ‘can easily find out how’ resulted in a larger R squared for PBC. It also caused ‘time consuming’ to become insignificant and so it was dropped. Dropping the power of control multiplication of ‘able to follow process’ and creating a path directly to intention rather than a precursor to PBC, modestly improved the R squared value of intention and pushed subjective norm over the 0.05 significance limit. The resulting improved model is shown in Figure 17. The associated parameter estimates appear in Table 25.

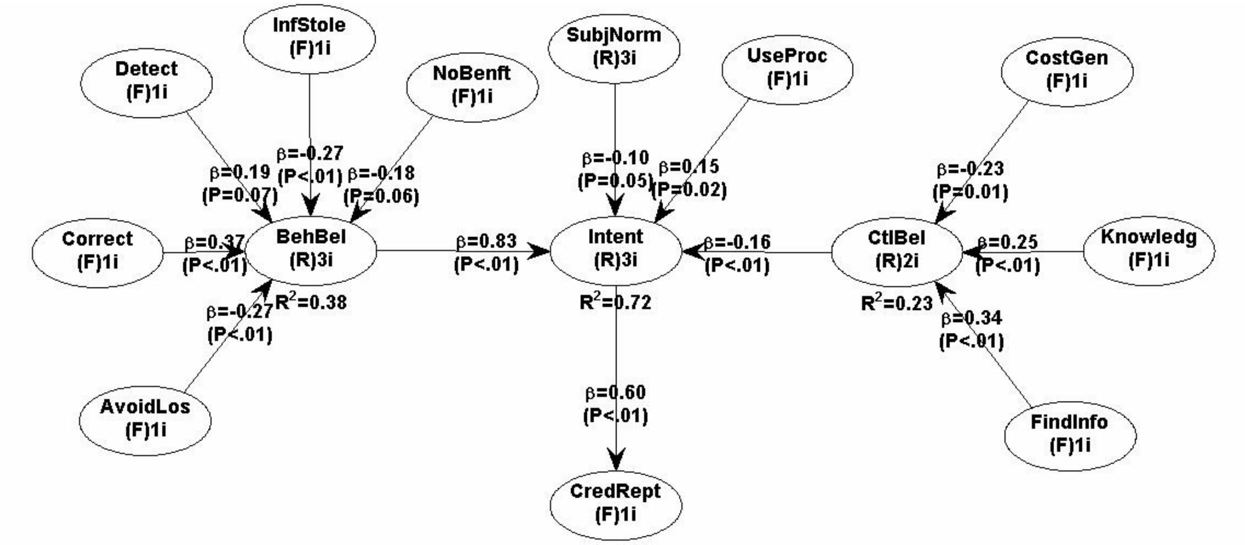


Figure 17 - Improved CredRept Model

These modifications suggest that at least some of the control beliefs act directly on intention without significant impact on the perceived behavioural control construct. The average path coefficient (APC) increased from 0.293 (p<0.001) in the original model to 0.304 (p<0.001) in the improved model and average R squared (ARS) increased from 0.404 (p<0.001) to 0.424 (p<0.001). Both measures relate to model quality and allow comparison of model fit with the same data.

Table 25 - Parameter Estimates for Improved CredRept Model

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to check credit report	0.601			
BehBel	Attitude towards getting credit report		0.828		
CtlBel	PBC towards getting my credit report		-0.161		
SubjNorm	Subjective norm		-0.101		
UseProc	Able to follow the process		0.154		
AvoidLos	Avoiding financial loss (g)			-0.269	
Correct	Correct mistakes			0.374	
Detect	Detect unauthorized use			0.192	
InfStole	Report will be stolen			-0.275	
NoBenft	Get no benefit			-0.176	
Knowledg	Requires a lot of knowledge (g)				0.249
CostGen	Costs a lot (g)				-0.233
FindInfo	Can easily find out how				0.337

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to check credit report	<0.001			
BehBel	Attitude towards getting credit report		<0.001		
CtlBel	PBC towards getting my credit report		0.003		
SubjNorm	Subjective norm		0.053		
UseProc	Able to follow the process		0.019		
AvoidLos	Avoiding financial loss (g)			0.002	
Correct	Correct mistakes			<0.001	
Detect	Detect unauthorized use			0.072	
InfStole	Report will be stolen			0.002	
NoBenft	Get no benefit			0.061	
Knowledg	Requires a lot of knowledge (g)				0.006
CostGen	Costs a lot (g)				0.014
FindInfo	Can easily find out how				0.003

Effect Size

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to check credit report	0.362			
BehBel	Attitude towards getting credit report		0.681		
CtlBel	PBC towards getting my credit report		0.001		
SubjNorm	Subjective norm		0.011		
UseProc	Able to follow the process		0.055		
AvoidLos	Avoiding financial loss (g)			0.007	
Correct	Correct mistakes			0.161	
Detect	Detect unauthorized use			0.070	
InfStole	Report will be stolen			0.064	
NoBenft	Get no benefit			0.076	
Knowledg	Requires a lot of knowledge (g)				0.040
CostGen	Costs a lot (g)				0.061
FindInfo	Can easily find out how				0.129

	Behaviour	Intention	Attitude	PBC
R Squared	0.362	0.725	0.379	0.231

The model still has one glaring flaw: the path coefficient from PBC to intent is significant (p = 0.003) and negative (-0.161). According to the hypothesis, increases in PBC are supposed to increase intention and not decrease it.

Of interest to practitioners are the findings on the specific beliefs that affect the attitude toward checking one's credit report. The belief in the ability to correct mistakes had more effect than the belief in the ability to detect unauthorized use. The belief that the information would be stolen had a significant negative effect on the attitude toward getting a credit report. While the belief that the credit report would provide no benefit was not quite significant at the 0.05 level (p=0.061), it does suggest that consumer education might ultimately improve performance of this behaviour.

7.2 Phase 2 Sub-sample Land Registry TPB

This section documents the results and discusses the sub-sample asked the questions specific to the 'monitoring agencies' component. These questions allowed analysis of the full land registry TPB model for the sub-sample. Note that only home owners (n=49) were analyzed.

7.2.1 Phase 2 Sub-sample Land Registry TPB - Results

Keeping only the paths and associated beliefs that have significant p values from the 'full' model in Appendix P, the model shown in Figure 18 emerges, with the key parameter estimates in Table 26.

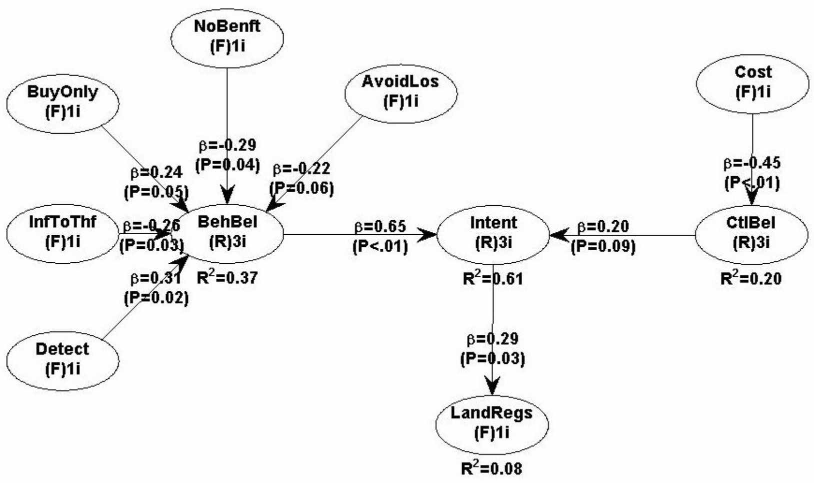


Figure 18 - TPB Model for LandRegs ('I check land registry office records at least once a year')

Table 26 - Parameter Estimates for LandRegs Model

LandReg Check land registry office records at least once a year

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to check with land registry office	0.289			
CtlBel	PBC towards checking land registry office		0.203		
BehBel	Attitude towards checking land registry office		0.646		
AvoidLos	Avoiding financial loss (g)			-0.221	
Detect	Detect any unauthorized mortgage			0.315	
InfToThf	Source of information to identity thieves			-0.265	
BuyOnly	Only needed when buying or selling			0.236	
NoBenft	Will receive no benefit			-0.287	
Cost	Costly				-0.448

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to check with land registry office	0.026			
CtlBel	PBC towards checking land registry office		0.091		
BehBel	Attitude towards checking land registry office		<0.001		
AvoidLos	Avoiding financial loss (g)			0.059	
Detect	Detect any unauthorized mortgage			0.015	
InfToThf	Source of information to identity thieves			0.034	
BuyOnly	Only needed when buying or selling			0.054	
NoBenft	Will receive no benefit			0.043	
Cost	Costly				<0.001

Table 26 cont'd

Effect Size

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to check with land registry office	0.084			
CtlBel	PBC towards checking land registry office		0.119		
BehBel	Attitude towards checking land registry office		0.494		
AvoidLos	Avoiding financial loss (g)			0.038	
Detect	Detect any unauthorized mortgage			0.089	
InfToThf	Source of information to identity thieves			0.079	
BuyOnly	Only needed when buying or selling			0.037	
NoBenft	Will receive no benefit			0.127	
Cost	Costly				0.201

	Behaviour	Intention	Attitude	PBC
R Squared	0.084	0.613	0.369	0.201

7.2.2 Phase 2 Sub-sample Land Registry TPB - Discussion

In this smaller sample, Hypotheses HT3 (attitude to intention) and HT9 (intention to behaviour) were supported as in the full sample but HT8, (PBC to intention) was not. HT10 (moderation of intention by PBC) and H5 (subjective norm to intention) were not supported. Only one of the general beliefs, ‘avoiding loss’ was significant and, as in the Credit Report model, the coefficient was negative, implying that HT2 (general behavioural beliefs to intention) was not supported. Of the five specific beliefs, four were significant or almost so although all the effect sizes were in the 'small' influence range (0.02-0.15), providing some support for HT1 (specific behavioural beliefs to intention). None of the general control beliefs had a significant effect on PBC, providing no support for HT7 (general control beliefs to PBC). Only one of the specific control beliefs had a significant effect on PBC but had a 'moderate' effect size, providing limited support to HT6 (specific control beliefs to PBC). The model failed to explain much of the variation in behaviour, with an R squared of only 0.084 and the influence of intention on behaviour was small.

Examination of the parameters and correlation coefficients suggested changes. PBC was dropped since it was not significant. The ‘requires a lot of knowledge’ control belief was added as a direct influence on intention. It and ‘requires diligence’ were added as moderators of intention on behaviour. The improved model is shown in Figure 19, with the associated parameter estimates in Table 27.

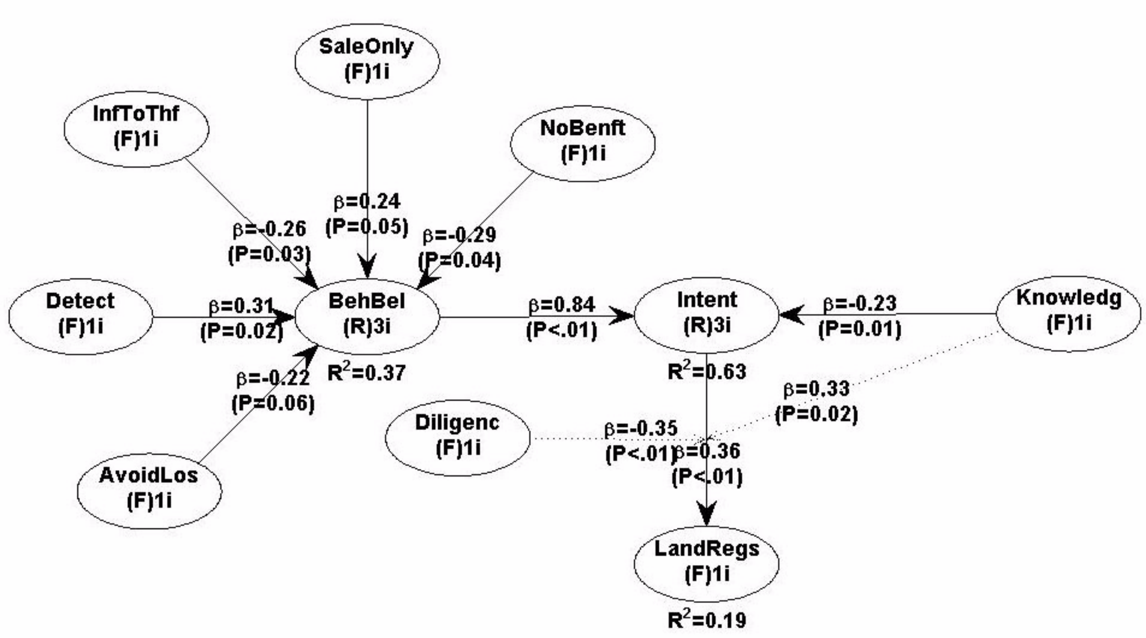


Figure 19 - Improved LandRegs Model

Table 27 - Parameter Estimates for Improved LandRegs Model

LandReg Check land registry office records at least once a year

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude
Intent	Intend to check with land registry office	0.362		
BehBel	Attitude towards checking land registry office		0.837	
Knowledg	Requires a lot of knowledge (g)		-0.228	
AvoidLos	Avoiding financial loss (g)			-0.221
Detect	Detect any unauthorized mortgage			0.315
InfToThf	Source of information to identity thieves			-0.265
BuyOnly	Only needed when buying or selling			0.236
NoBenft	Will receive no benefit			-0.287
Knowledg*Intent	Moderation of Intent by Knowledg	0.335		
Diligenc*Intent	Moderation of Intent by Diligenc	-0.354		

Table 27 cont'd

P Values

Variable	Description	Behaviour	Intention	Attitude
Intent	Intend to check with land registry office	0.006		
BehBel	Attitude towards checking land registry office		<0.001	
Knowledg	Requires a lot of knowledge (g)		0.015	
AvoidLos	Avoiding financial loss (g)			0.059
Detect	Detect any unauthorized mortgage			0.015
InfToThf	Source of information to identity thieves			0.034
BuyOnly	Only needed when buying or selling			0.054
NoBenft	Will receive no benefit			0.043
Knowledg*Intent	Moderation of Intent by Knowledg	0.023		
Diligenc*Intent	Moderation of Intent by Diligenc	0.003		

Effect Size

Variable	Description	Behaviour	Intention	Attitude
Intent	Intend to check with land registry office	0.105		
BehBel	Attitude towards checking land registry office		0.641	
Knowledg	Requires a lot of knowledge (g)		0.008	
AvoidLos	Avoiding financial loss (g)			0.038
Detect	Detect any unauthorized mortgage			0.089
InfToThf	Source of information to identity thieves			0.079
BuyOnly	Only needed when buying or selling			0.037
NoBenft	Will receive no benefit			0.127
Knowledg*Intent	Moderation of Intent by Knowledg	0.019		
Diligenc*Intent	Moderation of Intent by Diligenc	0.070		

	Behaviour	Intention	Attitude
R Squared	0.193	0.633	0.369

The R squared of behaviour increased from 0.084 to 0.193 and the R squared of intention increased marginally from 0.613 to 0.633. The overall model's APC increased from 0.323 (p<0.001) to 0.344 (p<0.001) and its ARS from 0.317 (p<0.001) to 0.398 (p<0.001).

Of practical interest are the specific beliefs that influenced the attitude toward checking the land registry office on a regular basis. Several of the beliefs that had a statistically significant impact on intent might be misguided; i.e., the beliefs that the information will be a source for identity thieves, that it is only needed when buying and selling a house, and that it will provide no benefit. These misinformed beliefs and the moderating effect of the belief that checking the land registry required a lot of knowledge had on the intention to actually check the land registry all suggest that education could have a significant effect on the intention and ultimately the performance of the behaviour.

7.3 Phase 2 Sub-sample Monitor Accounts TPB

This section documents the results and discusses the sub-sample (n=66) asked the questions specific to the 'monitoring accounts' component. These questions allowed analysis of the full 'monitoring accounts' TPB model for the sub-sample. The 'monitor accounts' component comprises two behaviours: ‘I monitor credit card accounts and activity at least once a month’ and ‘I monitor bank account balances and activity at least once a month’. In the full model in Appendix P, both behaviours were modeled as a single formative construct.

7.3.1 Phase 2 Sub-sample Monitor Accounts TPB - Results

Keeping only the paths and associated beliefs that had significant p values from the ‘full’ model, the model shown in Figure 20 emerges, with the key parameter estimates in Table 28.

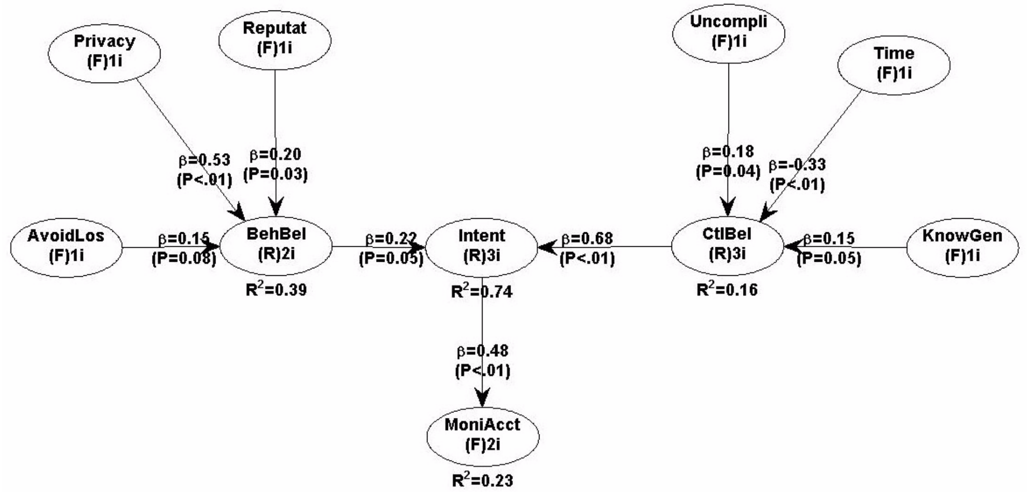


Figure 20 - TPB Model for MoniAcct ('I monitor my credit cards and bank accounts')

Table 28 - Parameter Estimates for MoniAcct Model

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to monitor bank accounts and credit cards	0.483			
BehBel	Attitude towards monitoring accounts and cards		0.223		
CtlBel	PBC towards monitoring accounts and cards		0.684		
AvoidLos	Avoiding financial loss (g)			0.151	
Privacy	Protecting my privacy (g)			0.527	
Reputat	Preventing the loss of my reputation (g)			0.202	
KnowGen	Requires a lot of knowledge (g)				0.154
Time	Takes too much time				-0.332
Uncompli	Easier if process is uncomplicated				0.180

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to monitor bank accounts and credit cards	<0.001			
BehBel	Attitude towards monitoring accounts and cards		0.052		
CtlBel	PBC towards monitoring accounts and cards		<0.001		
AvoidLos	Avoiding financial loss (g)			0.078	
Privacy	Protecting my privacy (g)			0.003	
Reputat	Preventing the loss of my reputation (g)			0.034	
KnowGen	Requires a lot of knowledge (g)				0.048
Time	Takes too much time				<0.001
Uncompli	Easier if process is uncomplicated				0.044

Effect Sizes

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to monitor bank accounts and credit cards	0.233			
BehBel	Attitude towards monitoring accounts and cards		0.161		
CtlBel	PBC towards monitoring accounts and cards		0.580		
AvoidLos	Avoiding financial loss (g)			0.052	
Privacy	Protecting my privacy (g)			0.304	
Reputat	Preventing the loss of my reputation (g)			0.031	
KnowGen	Requires a lot of knowledge (g)				0.021
Time	Takes too much time				0.109
Uncompli	Easier if process is uncomplicated				0.035
R Squared		0.233	0.741	0.387	0.165

7.3.1 Phase 2 Sub-sample Monitor Accounts TPB - Discussion

Compared to the other behaviours in this study, monitoring accounts is unusual in that PBC has more effect on intention than does attitude. Although attitude is slightly over the 0.05 level of significance, it was retained in the model since it was supported in the full sample. None of the beliefs specific to the behaviour had a significant effect on attitude, although three of the general behavioural beliefs had a significant or close to significant effect. HT1 (specific behaviour beliefs affect attitude) was therefore unsupported while HT2 (general behaviour beliefs affect attitude) was supported. HT3 (attitudes affect intention) was technically not supported in this smaller sample although it was in the larger sample. As in most other behaviours, H5 (subjective norm affects intention) was not supported. Only one of the general control beliefs, ‘requires a lot of knowledge’ had a significant effect on PBC, providing some support for HT7 (general control beliefs affect PBC). Two of the control beliefs specific to the behaviour, ‘takes too much time’ and ‘easier if the process is uncomplicated’ had significant effects on PBC, providing support for HT6 (specific control beliefs affect PBC). PBC had a significant effect on intent, providing support for HT8. Intention had a significant effect on performance of the behaviour (support for HT9) and HT10 (PBC moderation of the effect of intent on performance) was not supported.

The R squared for PBC was low at 0.165, implying that less than one-sixth of the variation was explained. Examination of the correlation matrix suggested improvements. Some control beliefs were returned to their ‘un-multiplied state’; that is, the control belief behaviour-specific items, ‘I get regular bank and credit card statements’ and ‘The process to monitor my bank accounts and credit cards is easy and uncomplicated’ and the general control item ‘I can easily find information on how to protect my personal identity information’ were not multiplied by their matching ‘power of control’ items. The component behaviours were split and the ‘difficult if jointly owned’ control belief was added as a moderator of the intent to ‘monitoring cards’ behaviour. The improved model is shown in Figure 21, with the associated parameter estimates in Table 29.

Using the ‘raw’ items as inputs to PBC, the R squared for PBC rose to 0.329. Adding the ‘difficult if jointly owned’ control belief as a moderator of the intent to ‘monitoring cards’ behaviour increased the overall ARS. APC basically stayed the same, going from 0.334 (p<0.001) to 0.330 (p<0.001), while ARS increased from 0.340 (p= 0.010) to 0.376 (p=0.008).

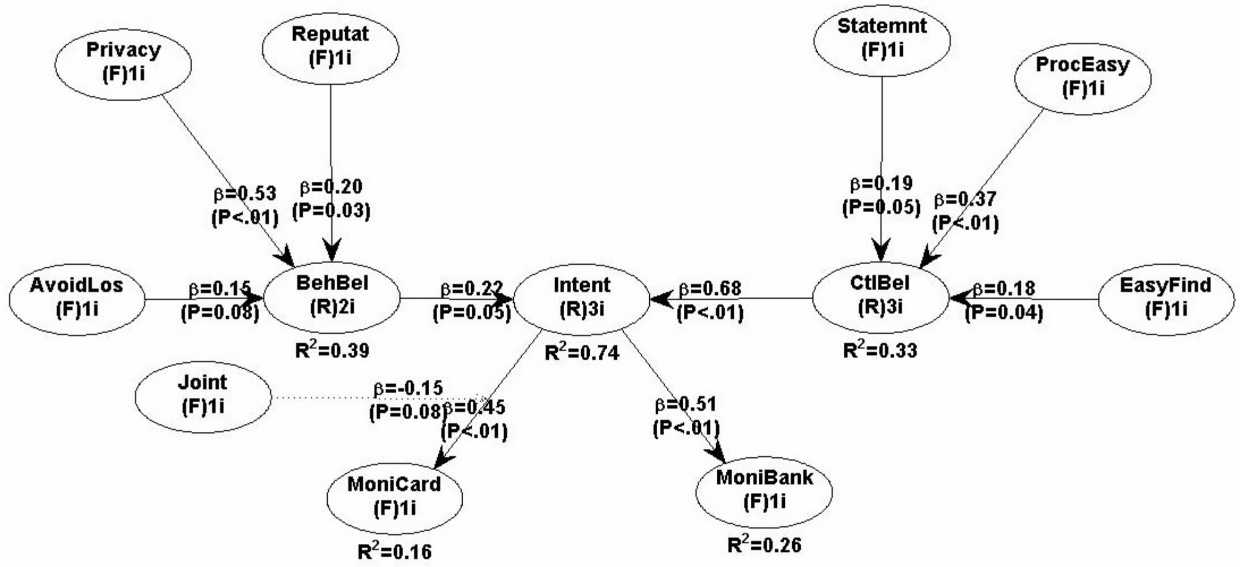


Figure 21 - Improved MoniAcct Model

Table 29 - Improved MoniAcct Model Parameter Estimates

MoniCard	I monitor my credit cards once a month
MoniBank	I monitor my bank accounts once a month

Path Coefficients

Variable	Description	Moni Card	Moni Bank	Intent	Attitude	PBC
Intent	Intent to monitor credit cards and bank accounts	0.450	0.509			
BehBel	Attitude towards monitoring credit cards and bank account			0.223		
CtlBel	PBC towards monitoring credit cards and bank account			0.684		
AvoidLos	Avoiding financial loss (g)				0.151	
Privacy	Protecting my privacy (g)				0.527	
Reputat	Preventing the loss of my reputation (g)				0.202	
EasyFind	Can easily find information on how to protect my identity info (g)					0.176
ProcEasy	Process to monitor my bank accounts and credit cards is easy					0.372
Statemnt	Get regular bank and credit card statements					0.186
Joint	Difficult if jointly owned					
Joint*Intent	Moderation of intention by joint	-0.145				

P Values

Variable	Description	Moni Card	Moni Bank	Intent	Attitude	PBC
Intent	Intent to monitor credit cards and bank accounts	<0.001	0.001			
BehBel	Attitude towards monitoring credit cards and bank account			0.052		
CtlBel	PBC towards monitoring credit cards and bank account			<0.001		
AvoidLos	Avoiding financial loss (g)				0.078	
Privacy	Protecting my privacy (g)				0.003	
Reputat	Preventing the loss of my reputation (g)				0.034	
EasyFind	Can easily find information on how to protect my identity info (g)					0.039
ProcEasy	Process to monitor my bank accounts and credit cards is easy					0.003
Statemnt	Get regular bank and credit card statements					0.053
Joint	Difficult if jointly owned					
Joint*Intent	Moderation of intention by joint	0.075				

Table 29 cont'd

Effect Sizes

Variable	Description	Moni Card	Moni Bank	Intent	Attitude	PBC
Intent	Intent to monitor credit cards and bank accounts	0.172	0.259			
BehBel	Attitude towards monitoring credit cards and bank account			0.161		
CtlBel	PBC towards monitoring credit cards and bank account			0.580		
AvoidLos	Avoiding financial loss (g)				0.052	
Privacy	Protecting my privacy (g)				0.304	
Reputat	Preventing the loss of my reputation (g)				0.031	
EasyFind	Can easily find information on how to protect my identity info (g)					0.066
ProcEasy	Process to monitor my bank accounts and credit cards is easy					0.195
Statemnt	Get regular bank and credit card statements					0.069
Joint	Difficult if jointly owned					
Joint*Intent	Moderation of intention by joint	0.009				
		Moni Card	Moni Bank	Intent	Attitude	PBC
R Squared		0.163	0.259	0.741	0.387	0.329

That the general behavioural beliefs figure so prominently in this model suggests that consumers identify monitoring their accounts and credit cards with preventing identity theft and detecting identity fraud. Unlike the credit report and land registry behaviours, monitoring accounts and cards seems to be a ‘motherhood’ issue, with almost all respondents indicating very positive attitudes. In fact, all of the key constructs, attitude, PCB, intention, and performance were highly skewed in the same direction (see Appendix K).

7.4 Phase 2 Sub-sample Physical Security TPB

This section documents the results and discusses the sub-sample (n=67) asked the questions specific to the 'physical security' component. These questions allowed analysis of the full 'physical security' TPB model for the sub-sample. The physical security component comprises three behaviours: ‘I use a locked mailbox for incoming mail’, ‘I shred financial or important documents before discarding them’ and 'I keep sensitive financial information in a secure location, such as a locked drawer or box'. Since the 'locked mailbox' behaviour did not load onto the same component in the principal components analysis, the three behaviours were modeled as individual endogenous variables.

7.4.1 Phase 2 Sub-sample Physical Security TPB - Results

The full model and associated parameter estimates are shown in Appendix P. Deleting the constructs with insignificant paths results in the model shown in Figure 22, with the attendant estimates shown in Table 30.

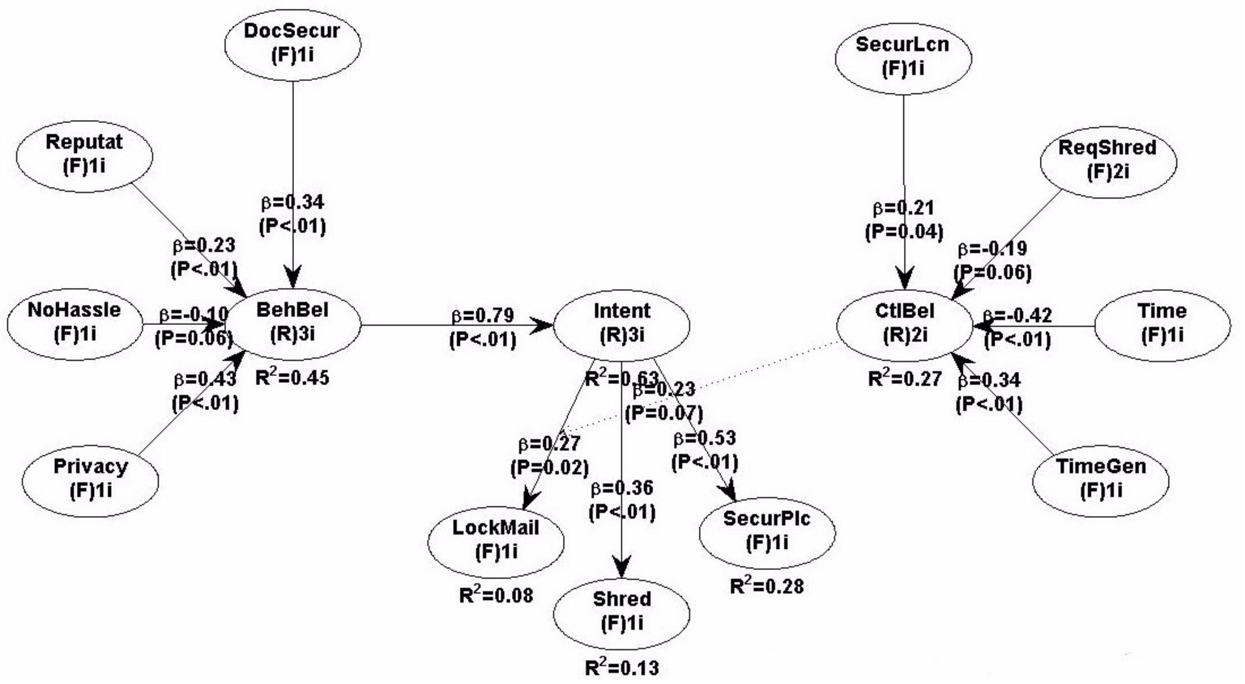


Figure 22 - TPB Model for PhysSec (Physical Security Behaviours)

Table 30 - Parameter Estimates for Model PhysSec Model

LockMail I use a locked mailbox for incoming mail
Shred I shred financial or important documents before discarding them
SecurPlc I keep sensitive financial information in a secure location

Path Coefficients

Variable	Description	LockMail	Shred	SecurPlc	Intention	Attitude	PBC
Intent	Intend to secure my documents	0.274	0.360	0.532			
BehBel	Attitude to securing documents				0.792		
Privacy	Protecting my privacy (g)					0.426	
NoHassle	Avoiding the hassle of fraud (g)					-0.105	
Reputat	Preventing loss of reputation (g)					0.234	
DocSecur	My identity info will be secure					0.337	
TimeGen	Takes a lot of time (g)						0.342
Time	Takes too much time						-0.415
ReqShred	Requires a shredder						-0.189
SecurLcn	Requires a secure location						0.211
CtlBel*Intent	Moderation of Intent by PBC	0.232					

Table 30 cont'd

P Values

Variable	Description	LockMail	Shred	SecurPlc	Intention	Attitude	PBC
Intent	Intend to secure my documents	0.020	<0.001	<0.001			
BehBel	Attitude to securing documents				<0.001		
Privacy	Protecting my privacy (g)					<0.001	
NoHassle	Avoiding the hassle of fraud (g)					0.065	
Reputat	Preventing loss of reputation (g)					0.007	
DocSecur	My identity info will be secure					0.001	
TimeGen	Takes a lot of time (g)						0.002
Time	Takes too much time						<0.001
ReqShred	Requires a shredder						0.061
SecurLcn	Requires a secure location						0.045
CtlBel*Intent	Moderation of Intent by PBC	0.068					

Effect Size

Variable	Description	LockMail	Shred	SecurPlc	Intention	Attitude	PBC
Intent	Intend to secure my documents	0.051	0.130	0.283			
BehBel	Attitude to securing documents				0.626		
Privacy	Protecting my privacy (g)					0.238	
NoHassle	Avoiding the hassle of fraud (g)					0.002	
Reputat	Preventing loss of reputation (g)					0.032	
DocSecur	My identity info will be secure					0.178	
TimeGen	Takes a lot of time (g)						0.072
Time	Takes too much time						0.142
ReqShred	Requires a shredder						0.009
SecurLcn	Requires a secure location						0.068
CtlBel*Intent	Moderation of Intent by PBC	0.030					
R Squared		0.081	0.130	0.283	0.626	0.451	0.273

7.4.2 Phase 2 Sub-sample Physical Security TPB - Discussion

Only one of the behavioural beliefs specific to physical security (‘My identity information will be secure’) was significant, providing some support for Hypothesis HT1 (specific behavioural beliefs to intent). Three of the general behavioural beliefs had significant or marginally significant effects on attitude. Again, the direction of influence for ‘avoid the hassle of fraud’ was unexpected. Given the other two significant general beliefs, ‘protecting my privacy’ and ‘preventing loss of reputation’, there was support for Hypothesis HT2 (general behavioural beliefs to intent). Attitude strongly affected intention, supporting HT3. Subjective norm was not significant, so H5 was not supported. When it comes to PBC, the opposite of the situation for attitude occurred. Only one of the general control beliefs was significant, whereas three of the specific control beliefs were significant or marginally significant. There was therefore limited support for HT7 (general control beliefs to PBC) and significant support for HT6 (specific control beliefs to PBC). HT8 (PBC affects intention) was not supported. As in all behaviours, HT9 (intention to behaviour) was supported. HT10 (PBC moderates intention to behaviour) was not supported except for the ‘locked mailbox’ behaviour where it was marginally insignificant.

Because PBC had no significant effect on intention in the TPB model, control beliefs had no ultimate effect on behaviour except as a moderator of the path from intention to the 'locked mailbox' behaviour. Furthermore, the R squared values for the three behaviours were not high. The addition of ‘takes too much time’ as an input to the ‘secure place’ behaviour increased its R squared from 0.283 to 0.322. The addition of ‘takes too much time’ and ‘requires a shredder’ to the ‘shred documents’ behaviour raised its R squared from 0.130 to 0.226. The revised model is shown in Figure 23, with the associated parameter estimates in Table 31.

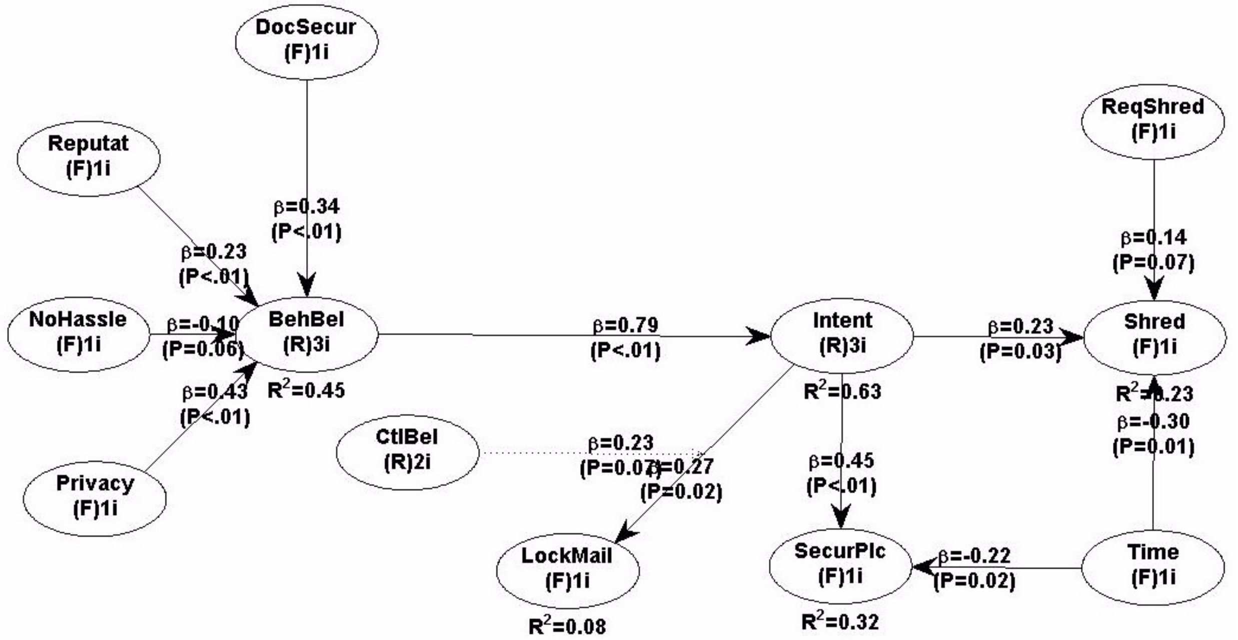


Figure 23 - Revised PhysSec Model

Table 31 - Revised PhysSec Model Parameter Estimates

LockMail	I use a locked mailbox for incoming mail
Shred	I shred financial or important documents before discarding them
SecurPlc	I keep sensitive financial information in a secure location

Path Coefficients

Variable	Description	LockMail	Shred	SecurPlc	Intention	Attitude
Intent	Intend to secure my documents	0.274	0.229	0.446		
BehBel	Attitude to securing documents				0.792	
Privacy	Protecting my privacy (g)					0.426
NoHassle	Avoiding the hassle of fraud (g)					-0.105
Reputat	Preventing loss of reputation (g)					0.234
DocSecur	My identity info will be secure					0.337
Time	Takes too much time		-0.296	-0.216		
ReqShred	Requires a shredder		0.138			
SecurLcn	Requires a secure location					
CtlBel*Intent	Moderation of Intent by PBC	0.232				

P Values

Variable	Description	LockMail	Shred	SecurPlc	Intention	Attitude
Intent	Intend to secure my documents	0.020	0.033	<0.001		
BehBel	Attitude to securing documents				<0.001	
Privacy	Protecting my privacy (g)					<0.001
NoHassle	Avoiding the hassle of fraud (g)					0.065
Reputat	Preventing loss of reputation (g)					0.007
DocSecur	My identity info will be secure					0.001
Time	Takes too much time		0.015	0.023		
ReqShred	Requires a shredder		0.073			
SecurLcn	Requires a secure location					
CtlBel*Intent	Moderation of Intent by PBC	0.068				

Effect Size

Variable	Description	LockMail	Shred	SecurPlc	Intention	Attitude
Intent	Intend to secure my documents	0.051	0.083	0.237		
BehBel	Attitude to securing documents				0.626	
Privacy	Protecting my privacy (g)					0.238
NoHassle	Avoiding the hassle of fraud (g)					0.002
Reputat	Preventing loss of reputation (g)					0.032
DocSecur	My identity info will be secure					0.178
Time	Takes too much time		0.118	0.085		
ReqShred	Requires a shredder		0.025			
SecurLcn	Requires a secure location					
CtlBel*Intent	Moderation of Intent by PBC	0.030				

	LockMail	Shred	SecurPlc	Intention	Attitude
R Squared	0.081	0.226	0.322	0.626	0.451

The addition of these control beliefs as direct influences on behaviour makes sense. PBC apparently had minimal influence on intention but at least some of the control beliefs did influence behaviour. The APC dropped slightly from 0.342 ($p<0.001$) to 0.310 ($p<0.001$) while ARS increased from 0.307 ($p<0.001$) to 0.341 ($p<0.001$).

It should be noted that the ‘locked mailbox’ behaviour was ‘orphaned’ in the principal components analysis on the current set of data and not grouped with the physical security behaviours as in Gilbert and Archer (2012). That realignment may explain its poor R squared value in the physical security model along with the fact that most Canadians do not get door-to-door mail delivery (Canada Post, 2013). While the influence of attitude on intention was strong as in most of the behaviours, the effect of intention on actually performing the behaviours was relatively weak. It is only by incorporating control beliefs as direct influences on behaviours that the explanation of the behaviours is increased. The practical lesson here is that individuals should be encouraged to act upon their intentions with regard to physical security and that control barriers such as access to a shredder and having a secure place to store sensitive documents need to be removed.

7.5 Phase 2 Sub-sample Password Security TPB

This section documents the results and discusses the sub-sample (n=67) asked the questions specific to the 'password security' component. These questions allowed analysis of the full 'password security' TPB model for the sub-sample. The password security component comprises two behaviours: '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.)' and 'I have different passwords for different applications or services'. The two behaviours were modeled as individual endogenous variables. There were some modifications made due to multicollinearity. Three of the PBC items dealing with factors that make password security difficult (‘Frequently changing my passwords makes them difficult to remember’, ‘Differing password standards in different applications make remembering passwords difficult' and 'Secure passwords are hard to remember') were combined into one formative construct.

7.5.1 Phase 2 Sub-sample Password Security TPB - Results

The full model in Appendix P includes all variables. Including only significant paths from the full model, the model in Figure 24 emerges. Table 32 shows the associated parameter estimates.

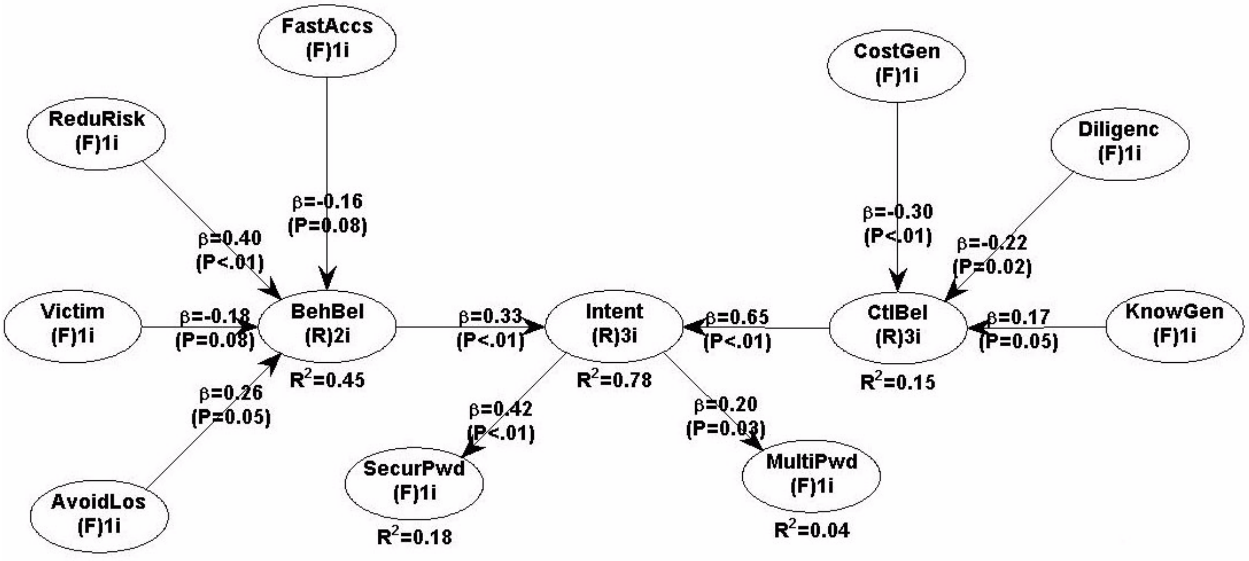


Figure 24 - TPB Model for Password Security

Table 32 - Password Security Model Parameter Estimates

SecurPwd	Use hard-to-break passwords
MultiPwd	Use different passwords for different applications

Path Coefficients

Variable	Description	SecurPwd	MultiPwd	Intention	Attitude	PBC
Intent	Intend to use secure passwords	0.425	0.200			
CtlBel	PBC towards getting my credit report			0.649		
BehBel	Attitude towards getting credit report			0.332		
AvoidLos	Avoiding financial loss (g)				0.263	
Victim	Will be the victim of identity crime (n)				-0.184	
ReduRisk	Reduce the risk of identity crime				0.403	
FastAcc	Online access will be slower				-0.159	
KnowGen	Requires a lot of knowledge (g)					0.171
Diligenc	Requires diligence (g)					-0.221
CostGen	Costs a lot (g)					-0.299

Table 32 cont'd

P Values

Variable	Description	SecurPwd	MultiPwd	Intention	Attitude	PBC
Intent	Intend to use secure passwords	<0.001	0.033			
CtlBel	PBC towards getting my credit report			<0.001		
BehBel	Attitude towards getting credit report			0.005		
AvoidLos	Avoiding financial loss (g)				0.055	
Victim	Will be the victim of identity crime (n)				0.079	
ReduRisk	Reduce the risk of identity crime				0.004	
FastAcc	Online access will be slower				0.077	
KnowGen	Requires a lot of knowledge (g)					0.046
Diligenc	Requires diligence (g)					0.019
CostGen	Costs a lot (g)					0.005

Effect Size

Variable	Description	SecurPwd	MultiPwd	Intention	Attitude	PBC
Intent	Intend to use secure passwords	0.180	0.040			
CtlBel	PBC towards getting my credit report			0.547		
BehBel	Attitude towards getting credit report			0.236		
AvoidLos	Avoiding financial loss (g)				0.128	
Victim	Will be the victim of identity crime (n)				0.090	
ReduRisk	Reduce the risk of identity crime				0.228	
FastAcc	Online access will be slower				0.004	
KnowGen	Requires a lot of knowledge (g)					0.010
Diligenc	Requires diligence (g)					0.048
CostGen	Costs a lot (g)					0.089

	SecurPwd	MultiPwd	Intention	Attitude	PBC
R Squared	0.180	0.040	0.783	0.450	0.147

7.5.2 Phase 2 Sub-sample Password Security TPB - Discussion

The hypotheses dealing with the connections between attitudes, PBC, intention, and behaviour (HT3, HT8 and HT9) were all supported. H5 (subjective norm on intention) and HT10 (moderation of intention on behaviours by PBC) were not supported. Only one of the general behavioural beliefs (avoiding financial loss) was significant, providing some support for Hypothesis HT2 (general behavioural beliefs affect attitude). Three of the five specific behavioural beliefs were significant or marginally significant at the 0.05 level, providing some support for HT1 (specific behavioural beliefs affect attitude). Unexpectedly, none of the specific control beliefs had a significant effect on PBC, providing no support for Hypothesis HT6. The only control beliefs with significant effects on PBC were general control beliefs, which provide support for HT7.

The very poor R squared for MultiPwd ('I use different passwords for different applications') is possibly due to the wording of the items used to directly measure intent. The wording was ‘I intend to use secure passwords’ rather than the more generic ‘I intend to practice password security’. The direct measure of intent may have then been skewed toward the ‘I use hard-to-break passwords’ rather than the ‘I have different passwords for different applications or services’ behaviour items. The model has other deficiencies. It is difficult to believe that none of the specific control beliefs such as ‘Frequently changing my passwords makes them difficult to remember’ or ‘Secure passwords are hard to remember’ have no bearing on password behaviour.

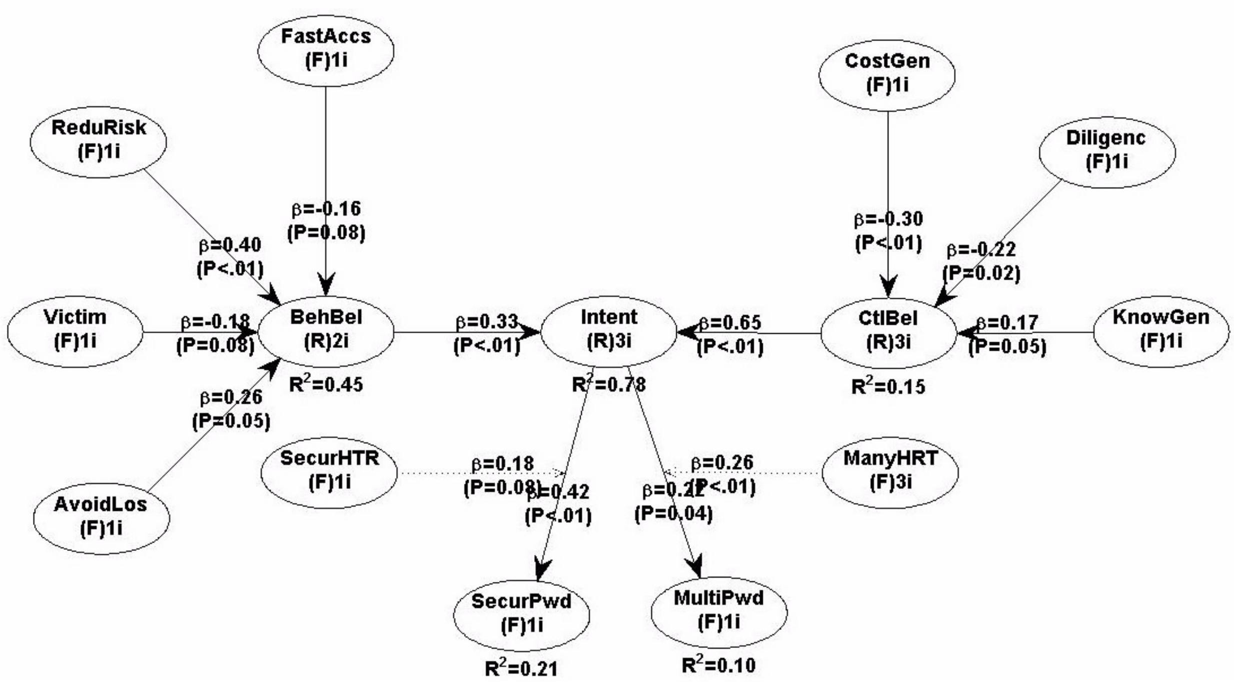


Figure 25 - Revised Password Security Model

Table 33 - Parameter Estimates for Revised Password Security Model

SecurPwd	Use hard-to-break passwords
MultiPwd	Use different passwords for different applications

Path Coefficients

Variable	Description	SecurPwd	MultiPwd	Intention	Attitude	PBC
Intent	Intend to use secure passwords	0.424	0.220			
CtlBel	PBC towards securing passwords			0.649		
BehBel	Attitude towards securing passwords			0.332		
AvoidLos	Avoiding financial loss (g)				0.263	
Victim	Will be the victim of identity crime (n)				-0.184	
ReduRisk	Reduce the risk of identity crime				0.403	
FastAcc	Online access will be slower				-0.159	
KnowGen	Requires a lot of knowledge (g)					0.171
Diligenc	Requires diligence (g)					-0.221
CostGen	Costs a lot (g)					-0.299
SecurHTR	Secure passwords are hard to remember*					
ManyHTR	Different passwords are hard to remember					
SecurHTR*Intent	Moderation of Intent by SecurHTR	0.181				
ManyHTR*Intent	Moderation of Intent by ManyHTR		0.256			

P Values

Variable	Description	SecurPwd	MultiPwd	Intention	Attitude	PBC
Intent	Intend to use secure passwords	<0.001	0.037			
CtlBel	PBC towards securing passwords			<0.001		
BehBel	Attitude towards securing passwords			0.005		
AvoidLos	Avoiding financial loss (g)				0.055	
Victim	Will be the victim of identity crime (n)				0.079	
ReduRisk	Reduce the risk of identity crime				0.004	
FastAcc	Online access will be slower				0.077	
KnowGen	Requires a lot of knowledge (g)					0.046
Diligenc	Requires diligence (g)					0.019
CostGen	Costs a lot (g)					0.005
SecurHTR	Secure passwords are hard to remember*					
ManyHTR	Different passwords are hard to remember					
SecurHTR*Intent	Moderation of Intent by SecurHTR	0.084				
ManyHTR*Intent	Moderation of Intent by ManyHTR		0.002			

Effect Size

Variable	Description	SecurPwd	MultiPwd	Intention	Attitude	PBC
Intent	Intend to use secure passwords	0.105	0.044			
CtlBel	PBC towards securing passwords			0.114		
BehBel	Attitude towards securing passwords			0.126		
AvoidLos	Avoiding financial loss (g)				0.162	
Victim	Will be the victim of identity crime (n)				0.129	
ReduRisk	Reduce the risk of identity crime				0.145	
FastAcc	Online access will be slower				0.110	
KnowGen	Requires a lot of knowledge (g)					0.100
Diligenc	Requires diligence (g)					0.104
CostGen	Costs a lot (g)					0.113
SecurHTR	Secure passwords are hard to remember*					
ManyHTR	Different passwords are hard to remember					
SecurHTR*Intent	Moderation of Intent by SecurHTR	0.130				
ManyHTR*Intent	Moderation of Intent by ManyHTR		0.061			

	SecurPwd	MultiPwd	Intention	Attitude	PBC
R Squared	0.213	0.105	0.783	0.450	0.147

* Combined items due to multicollinearity

Frequently changing my passwords makes them difficult to remember
Differing password standards in different applications make remembering passwords difficult
Secure passwords are hard to remember

The revised model is the same as the TPB model, with the addition of a moderator to each of the paths from intention to the two behaviours. SecurHTR, the formative construct formed from three of the specific control beliefs, moderates the path to the ‘hard-to-break passwords’ behaviour and the ‘different passwords’ control belief moderates the path to ‘different passwords for different applications’ behaviour. The revised model is shown in Figure 25, with the parameter estimates in Table 33.

The R squared for ‘hard-to-break passwords’ increases from 0.180 to 0.213 and that for ‘different passwords’ increases from 0.040 to 0.105. APC decreases slightly from 0.300 ($p<0.001$) to 0.289 ($p<0.001$) and ARS increases from 0.320 ($p<0.001$) to 0.339 ($p<0.001$).

While the revised model improved the R squared estimates for the two behaviours, the values were still low, indicating that much of the variation in the behaviours was unexplained. Password security is another ‘motherhood’ issue, with the vast majority having a positive attitude and intention (see Appendix K). There is a gap, however, between intention and behaviour performance that is only partially explained by the moderators in the revised model. In the qualitative input, password security figures prominently, so it is clearly an issue for consumers.

7.6 Phase 2 Sub-sample Risky Behaviours - Click on Link in an E-mail TPB

The next three sections document the results and discusses the sub-sample (n=78) asked the questions specific to the 'risky behaviours' component. The three 'risky' behaviours (clicking on a link in an e-mail, giving personal information over the phone, and using 'remember my password') are different than the other behaviours in that they represent behaviours to avoid in preventing identity theft rather than behaviours that proactively prevent identity theft or detect identity fraud. The risky behaviours are all convenient and easy to use but carry an added risk of victimization. Since they have little in common, other than they are risky, each was dealt with in a separate model documented in the following three sections.

Section 7.6 describes the results and discusses the 'I respond to a business by clicking on a link in an e-mail' behaviour.

7.6.1 Phase 2 Sub-sample Risky Behaviours - Click on Link in an E-mail TPB - Results

The reduced model for clicking on a link in an e-mail based on only significant paths from the full model in Appendix P is shown in Figure 26. The associated parameter estimates are in Table 34.

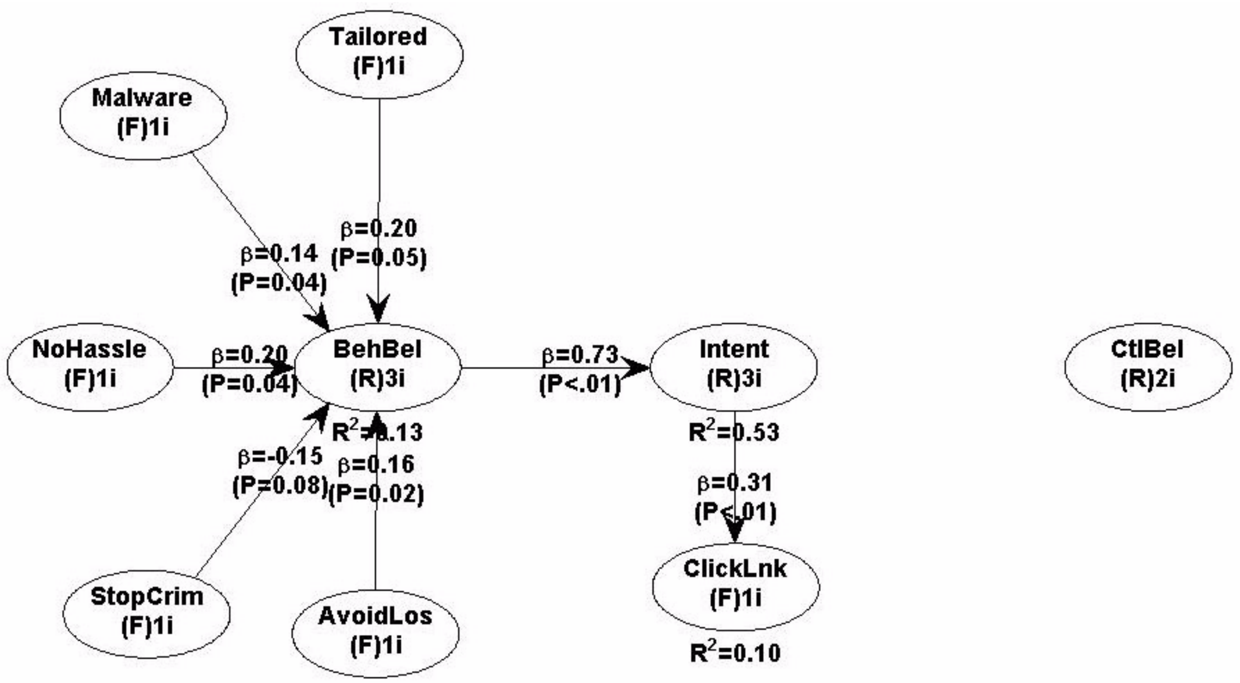


Figure 26 - TPB Model for ClickLnk ('I respond to a business by clicking on a link in an e-mail')

Table 34 - Parameter Estimates for ClickLnk Model

ClickLnk I respond to a business by clicking on a link in an e-mail

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude
Intent	Intend to click on a link in an e-mail	0.311		
BehBel	Attitude towards clicking on a link		0.730	
AvoidLos	Avoiding financial loss (g)			0.159
StopCrim	Stopping criminal activity (g)			-0.154
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.200
Malware	Will be the victim of malware			0.143
Tailored	Get information tailored to me			0.195

Table 34 cont'd

P Values

Variable	Description	Behaviour	Intention	Attitude
Intent	Intend to click on a link in an e-mail	0.006		
BehBel	Attitude towards clicking on a link		<0.001	
AvoidLos	Avoiding financial loss (g)			0.017
StopCrim	Stopping criminal activity (g)			0.083
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.038
Malware	Will be the victim of malware			0.044
Tailored	Get information tailored to me			0.046

Effect Size

Variable	Description	Behaviour	Intention	Attitude
Intent	Intend to click on a link in an e-mail	0.097		
BehBel	Attitude towards clicking on a link		0.533	
AvoidLos	Avoiding financial loss (g)			0.013
StopCrim	Stopping criminal activity (g)			0.020
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.038
Malware	Will be the victim of malware			0.019
Tailored	Get information tailored to me			0.041

	Behaviour	Intention	Attitude
R Squared	0.097	0.533	0.131

7.6.2 Phase 2 Sub-Sample Risky Behaviours - Click on Link in an E-mail TPB - Discussion

The paths between attitude, intention and behaviour were all significant, providing support for Hypotheses HT3 and HT9. PBC did not have a significant path to intent or a moderating effect on the path from intention to behaviour, so Hypotheses HT8 and HT10 were not supported. Three of the general behavioural beliefs had significant or marginally significant effects on attitude. The signs of the path coefficients are suspect, however. Since clicking on a link in an e-mail is a risky behaviour, one would expect that increasing the behaviour would decrease the benefits of identity theft protection, so the signs of the path coefficients should be negative. This is the case for only the ‘stopping criminal activity’ belief. These coefficients did not constitute support for HT2. Two of the specific behavioural beliefs had significant effects on attitude. The ‘will be a victim of malware’ belief should have decreased the attitude toward the behaviour but the coefficient was positive. Support for Hypothesis HT1 cannot, therefore, be established. None of the general specific control beliefs had significant path coefficients to PBC. Hypotheses

HT6 and HT7 had no support. The effect of subjective norm on intent was not significant, so H5 was unsupported. On the whole, the model was not very successful. The R squared values of behaviour and attitude were small, PBC and its associated beliefs were irrelevant, and with the exception of the effect of attitude on intention, the effect sizes were all very small.

By adding a general control belief, ‘takes too much time’ as an input to intent, the R squared of intent increased marginally. Since the risky behaviours could be characterized as ‘expedience over safety’, a negative coefficient to intention makes sense. The addition of the ‘I will not be a victim if I just open and then close the link’ belief as a moderator of the path between intention and performance is also logical and increases the R squared. The improved model is illustrated in Figure 27, with its parameter estimates in Table 35.

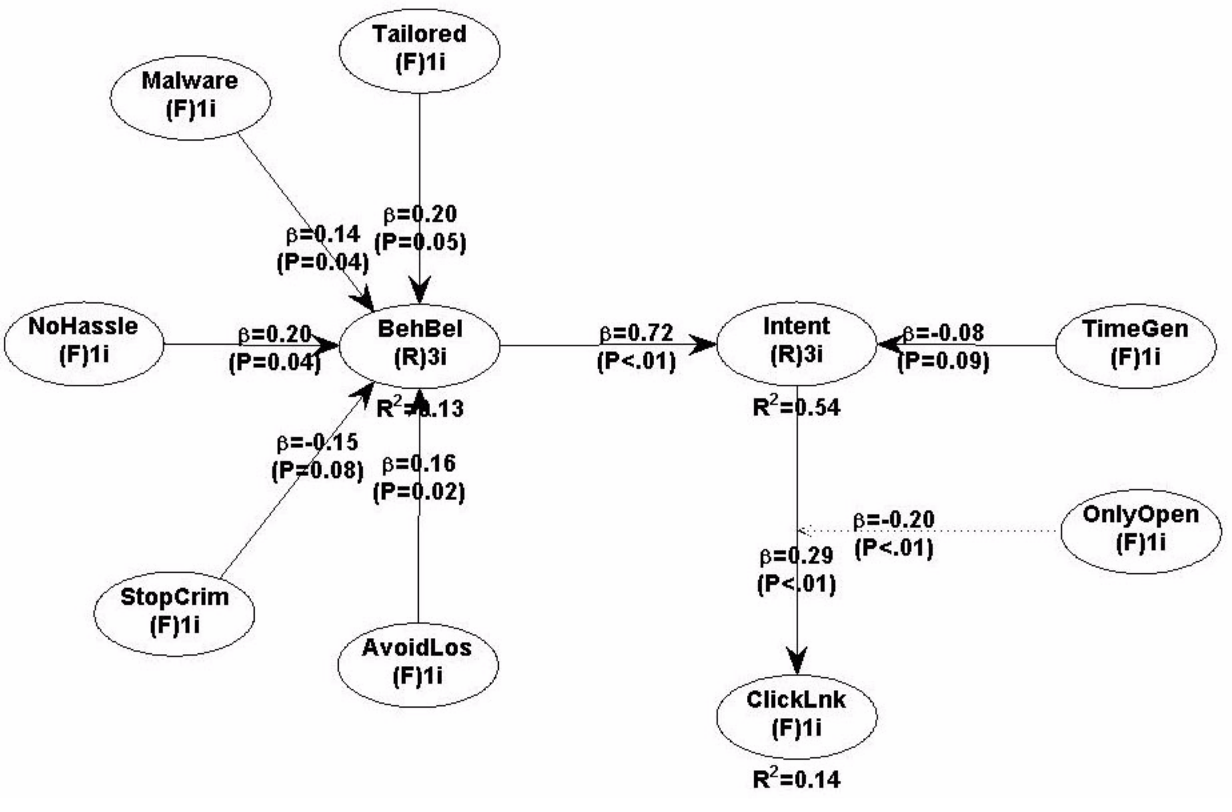


Figure 27 - Improved ClickLnk model

Table 35 - Parameter Estimates for Improved ClickLnk Model

ClickLnk I respond to a business by clicking on a link in an e-mail

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude
Intent	Intend to click on a link in an e-mail	0.290		
BehBel	Attitude towards clicking on a link		0.720	
AvoidLos	Avoiding financial loss (g)			0.159
StopCrim	Stopping criminal activity (g)			-0.154
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.200
Malware	Will be the victim of malware			0.143
Tailored	Get information tailored to me			0.195
TimeGen	Takes a lot of time (g)		-0.078	
OnlyOpen	Will not be the victim if I just open and close			
OnlyOpen*Intent	Moderation of Intent by OnlyOpen	-0.204		

P Values

Variable	Description	Behaviour	Intention	Attitude
Intent	Intend to click on a link in an e-mail	0.007		
BehBel	Attitude towards clicking on a link		<0.001	
AvoidLos	Avoiding financial loss (g)			0.017
StopCrim	Stopping criminal activity (g)			0.083
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.038
Malware	Will be the victim of malware			0.044
Tailored	Get information tailored to me			0.046
TimeGen	Takes a lot of time (g)		0.091	
OnlyOpen	Will not be the victim if I just open and close			
OnlyOpen*Intent	Moderation of Intent by OnlyOpen	0.009		

Effect Size

Variable	Description	Behaviour	Intention	Attitude
Intent	Intend to click on a link in an e-mail	0.090		
BehBel	Attitude towards clicking on a link		0.526	
AvoidLos	Avoiding financial loss (g)			0.013
StopCrim	Stopping criminal activity (g)			0.020
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.038
Malware	Will be the victim of malware			0.019
Tailored	Get information tailored to me			0.041
TimeGen	Takes a lot of time (g)		0.014	
OnlyOpen	Will not be the victim if I just open and close			
OnlyOpen*Intent	Moderation of Intent by OnlyOpen	0.048		

	Behaviour	Intention	Attitude
R Squared	0.138	0.539	0.131

By adding the general control belief, ‘takes too much time’ as an input to intent, the R squared of intent increased marginally from 0.533 to 0.539. The addition of the ‘I will not be a victim if I just open and then close the link' belief as a moderator of the path between intention and performance increased the R squared from 0.097 to 0.138. The APC dropped somewhat from 0.271 (p<0.001) to 0.238 (p<0.001) while the ARS increased from 0.254 (p<0.001) to 0.270 (p<0.001).

Practitioners should note that the strength of the belief that just opening and closing a link causes no harm had a measurable impact. Education to the contrary is indicated.

7.7 Phase 2 Sub-sample Risky Behaviours - Give Personal Information over the Phone TPB

This section provides the results and discusses the 'risky' behaviour 'I give personal information over the phone to people who do surveys, or people offering products or services at special prices' for the sub-sample (n=78) that completed the 'risky behaviour' questions, which allows the complete TPB model to be examined.

7.7.1 Phase 2 Sub-sample Risky Behaviours - Give Personal Information over the Phone TPB - Results

Removing insignificant paths from the full model shown in Appendix P leaves the model shown in Figure 28, with the associated parameter estimates in Table 36.

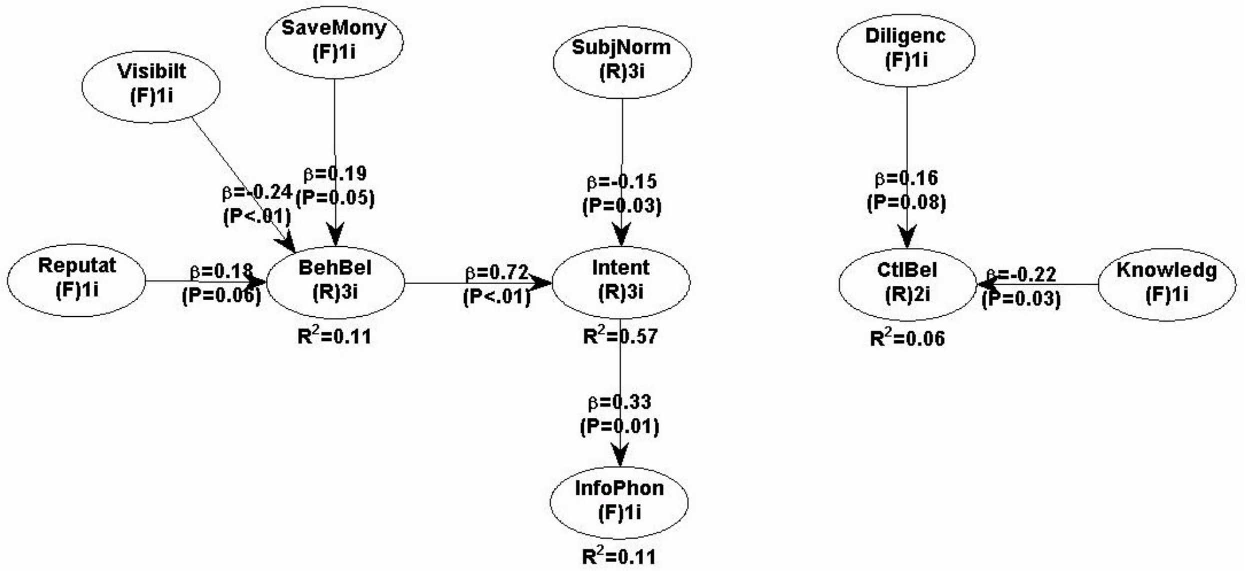


Figure 28 - TPB Model of InfoPhon ('I give personal information over the phone')

Table 36 - InfoPhon Parameter Estimates

InfoPho I give personal information over the phone

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to give personal information over the phone	0.333			
BehBel	Attitude to giving personal info over the phone		0.721		
SubjNorm	Subjective norm		-0.155		
Reputat	Preventing the loss of my reputation (g)			0.182	
Visabilt	Reducing my online visibility (g)			-0.243	
SaveMon	Get a good deal			0.190	
Knowledg	Requires a lot of knowledge (g)				-0.222
Diligenc	Requires diligence (g)				0.164

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to give personal information over the phone	0.014			
BehBel	Attitude to giving personal info over the phone		<0.001		
SubjNorm	Subjective norm		0.027		
Reputat	Preventing the loss of my reputation (g)			0.056	
Visabilt	Reducing my online visibility (g)			0.007	
SaveMon	Get a good deal			0.051	
Knowledg	Requires a lot of knowledge (g)				0.030
Diligenc	Requires diligence (g)				0.083

Effect Size

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to give personal information over the phone	0.111			
BehBel	Attitude to giving personal info over the phone		0.531		
SubjNorm	Subjective norm		0.035		
Reputat	Preventing the loss of my reputation (g)			0.028	
Visabilt	Reducing my online visibility (g)			0.054	
SaveMon	Get a good deal			0.034	
Knowledg	Requires a lot of knowledge (g)				0.041
Diligenc	Requires diligence (g)				0.018

	Behaviour	Intention	Attitude	PBC
R Squared	0.111	0.566	0.115	0.059

7.7.2 Phase 2 Sub-sample Risky Behaviours - Give Personal Information over the Phone TPB - Discussion

As in all other behaviours, the path between attitude and intention was strong, providing support for Hypothesis HT3. This is one of the few behaviours where subjective norm had a significant effect on intention but the direction was opposite what was expected. H5 was therefore unsupported. The relation between PBC and intention was not significant nor was the moderation of intent by PBC, so Hypotheses HT8 and HT10 were unsupported. Two of the general behavioural beliefs were statistically significant but suspect. ‘Preventing the loss of my reputation’ would be expected to have a negative coefficient, since giving out information on the phone is more likely to damage one's reputation than enhance it. ‘Reducing my online visibility’ should have no relation to telephone activity. Hypothesis HT2 was therefore not supported. The only specific behaviour belief that had statistical significance was ‘get a good deal’, providing some support for Hypothesis HT1. Two of the general control beliefs were statistically relevant.

The ‘requires a lot of knowledge’ belief makes some sense as an influence on PBC since the coefficient was negative. The coefficient of ‘requires diligence’ was positive, however, suggesting that individuals who believe that identity theft prevention requires diligence are more likely to engage in the risky behaviour of giving out personal information over the phone. Taken together, these two beliefs did not constitute support for Hypothesis HT7. None of the specific control beliefs were statistically significant, so HT6 is not supported. The path between intention and behaviour was statistically significant, supporting Hypothesis HT9.

The model was not particularly successful: many of the hypotheses were unsupported, all of the effect sizes were small for the beliefs, and the R squared values for behaviour and PBC were particularly low. Furthermore, some of the beliefs that might have been expected to be significant were not. For example, if the consumer makes the call, then the identity of the recipient is known and that is likely to reduce the risk. To improve the model, some of the control beliefs were included as direct influences on intention. These additions were substantiated by support for these beliefs from the Phase 1 exploratory survey and correlations from the Phase 2 quantitative survey. 'Diligence' was included as a direct path to behaviour because it originally had a significant effect on PBC but had no ultimate effect on behaviour since the effect PBC was insignificant. The improved model is shown in Figure 29, with associated parameter estimates in Table 37.

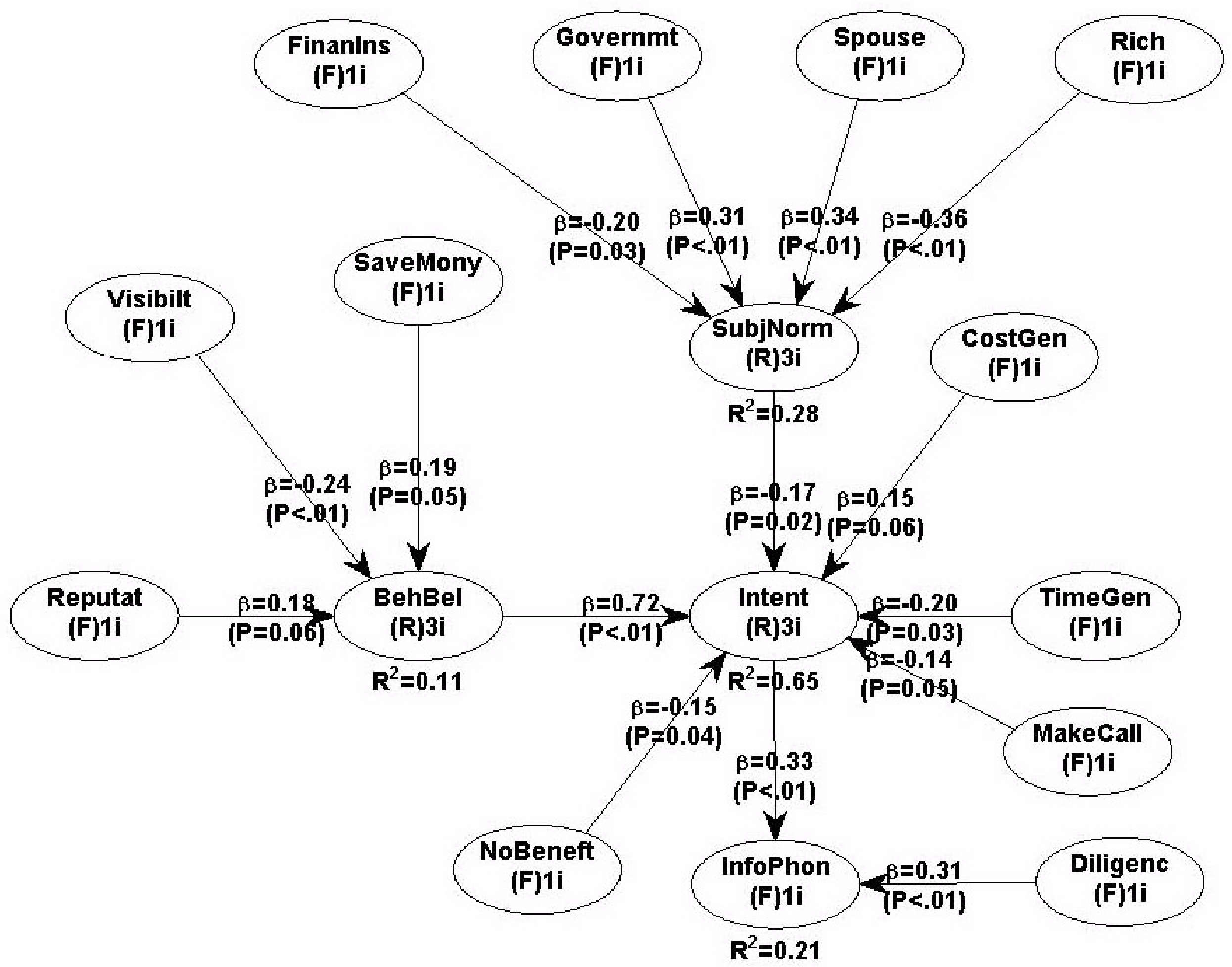


Figure 29 - Improved InfoPhon Model

Table 37 - Parameter Estimates for Improved InfoPhon Model

InfoPho I give personal information over the phone

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	Subj Norm
Intent	Intend to give personal information over the phone	0.335			
Diligenc	Requires diligence (g)	0.314			
BehBel	Attitude to giving personal info over the phone		0.716		
SubjNorm	Subjective norm		-0.170		
TimeGen	Takes a lot of time (g)		-0.201		
CostGen	Costs a lot (g)		0.151		
MakeCall	Only if I make the call		-0.137		
NoBeneft	Will receive no benefit		-0.153		
Reputat	Preventing the loss of my reputation (g)			0.182	
Visabilt	Reducing my online visibility (g)			-0.243	
SaveMony	Get a good deal			0.190	
FinanIns	Financial Institutions				-0.202
Governmt	Government				0.307
Spouse	Spouse				0.337
Rich	Rich people				-0.363

Table 37 cont'd

P Values

Variable	Description	Behaviour	Intention	Attitude	Subj Norm
Intent	Intend to give personal information over the phone	0.006			
Diligenc	Requires diligence (g)	0.003			
BehBel	Attitude to giving personal info over the phone		<0.001		
SubjNorm	Subjective norm		0.022		
TimeGen	Takes a lot of time (g)		0.025		
CostGen	Costs a lot (g)		0.056		
MakeCall	Only if I make the call		0.050		
NoBeneft	Will receive no benefit		0.037		
Reputat	Preventing the loss of my reputation (g)			0.056	
Visabilt	Reducing my online visibility (g)			0.007	
SaveMony	Get a good deal			0.051	
FinanIns	Financial Institutions				0.033
Governmt	Government				0.007
Spouse	Spouse				<0.001
Rich	Rich people				0.001

Effect Size

Variable	Description	Behaviour	Intention	Attitude	Subj Norm
Intent	Intend to give personal information over the phone	0.111			
Diligenc	Requires diligence (g)	0.098			
BehBel	Attitude to giving personal info over the phone		0.527		
SubjNorm	Subjective norm		0.038		
TimeGen	Takes a lot of time (g)		0.034		
CostGen	Costs a lot (g)		0.001		
MakeCall	Only if I make the call		0.028		
NoBeneft	Will receive no benefit		0.024		
Reputat	Preventing the loss of my reputation (g)			0.028	
Visabilt	Reducing my online visibility (g)			0.054	
SaveMony	Get a good deal			0.034	
FinanIns	Financial Institutions				0.000
Governmt	Government				0.039
Spouse	Spouse				0.118
Rich	Rich people				0.121

	Behaviour	Intention	Attitude	Subj Norm
R Squared	0.209	0.652	0.115	0.277

The inclusion of the significant normative beliefs for this smaller sample raises some interesting differences from the normative beliefs of the full sample. 'Co-workers', 'youths', 'parents' and 'criminals' became insignificant and 'government' and 'rich people' became significant, with only 'financial institutions' and 'spouse' significant in both samples. The coefficients of both 'financial institutions' and 'rich people' are both negative, suggesting that these two groups are mistrusted.

The intention R squared increased moderately from 0.566 to 0.652 while that of behaviour increased from 0.111 to 0.209. APC declined slightly from 0.271 (p<0.001) to 0.238 (p<0.001) while ARS increased from 0.254 (p<0.001) to 0.270 (p<0.001).

As a 'risky' behaviour, giving personal information over the phone is an expedient one. It is, however, slightly different from the other two 'risky' behaviours in that control is more of a factor. Whether one makes the call, the call is for a survey or a sales call, or the recipient has call display are all circumstances that could conceivably affect the behaviour. To properly use TPB in this case, the behaviour should perhaps be more specific in line with the consistency principal of TPB (Ajzen and Fishbein, 1980; Ajzen, 2005). For example, a behavioural item could have been 'I give personal information over the phone to telephone surveys when they call'.

Of practical interest is the finding that 'getting a good deal' was a significant influence on a positive attitude toward giving out personal information over the phone. Consumers need to be made aware of the potential risks they face in their quest for a 'bargain'.

7.8 Phase 2 Sub-sample Risky Behaviours - Use ‘Remember My Password’ TPB

This section provides the results and discusses the 'risky' behaviour 'I select "remember my card number" or "remember my password" for online log-ins' for the sub-sample (n=78) that completed the 'risky behaviour' questions, which allows the complete TPB model to be examined.

7.8.1 Phase 2 Sub-sample Risky Behaviours - Use ‘Remember My Password’ TPB - Results

The significant paths and variables from the full model in Appendix P are shown in Figure 30 and Table 38.

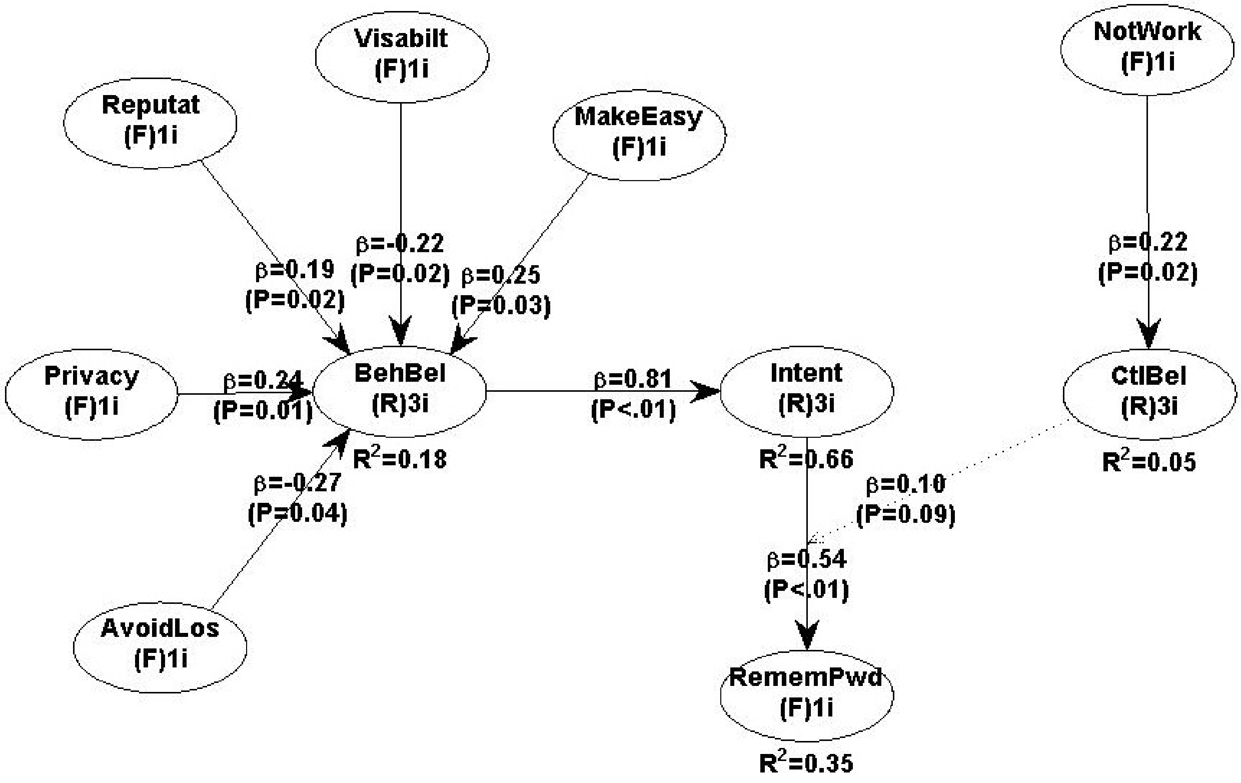


Figure 30 - TPB Model for RememPwd ('I select "remember my password" for online log-ins')

Table 38 - Parameter Estimates for TPB Model for RememPwd Model

RememPwd I select 'remember my card number' or 'remember my password' for online log-ins

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to use 'remember my password	0.542			
BehBel	Attitude to using 'remember my password'		0.813		
AvoidLos	Avoiding financial loss (g)			-0.268	
Privacy	Protecting my privacy (g)			0.240	
Reputat	Preventing the loss of my reputation (g)			0.193	
Visabilt	Reducing my online visibility (g)			-0.217	
MakeEasy	Web sites are easier to use			0.252	
NotWork	Does not always work				0.222
CtlBel*Intent	Moderation of intent by PBC	0.102			

Table 38 cont'd

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to use 'remember my password'	<0.001			
BehBel	Attitude to using 'remember my password'		<0.001		
AvoidLos	Avoiding financial loss (g)			0.043	
Privacy	Protecting my privacy (g)			0.014	
Reputat	Preventing the loss of my reputation (g)			0.025	
Visabilt	Reducing my online visibility (g)			0.020	
MakeEasy	Web sites are easier to use			0.029	
NotWork	Does not always work				0.024
CtlBel*Intent	Moderation of intent by PBC	0.094			

Effect Size

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to use 'remember my password'	0.318			
BehBel	Attitude to using 'remember my password'		0.660		
AvoidLos	Avoiding financial loss (g)			0.061	
Privacy	Protecting my privacy (g)			0.017	
Reputat	Preventing the loss of my reputation (g)			0.031	
Visabilt	Reducing my online visibility (g)			0.026	
MakeEasy	Web sites are easier to use			0.042	
NotWork	Does not always work				0.049
CtlBel*Intent	Moderation of intent by PBC	0.034			

	Behaviour	Intention	Attitude	PBC
R Squared	0.352	0.660	0.178	0.049

7.8.2 Phase 2 Sub-sample Risky Behaviours - Use ‘Remember My Password’ TPB - Discussion

The paths from attitude to intention and from intention to behaviour were both significant, supporting Hypotheses HT3 and HT9. The path from PBC to intention was not significant, providing no support for Hypothesis HT8. The moderation of the path from intention to behaviour by PBC was marginally significant, providing limited support for Hypothesis HT10. Hypothesis H5 was not supported, since the path from subjective norm to intention was not significant. Four of the general behavioural beliefs had significant paths to attitude but the signs of the coefficients were suspect. Since using 'remember my password' is a risky behaviour, the expectation was that the signs of the coefficients linking these beliefs with attitude would be negative, as was the case for 'avoiding financial loss'. Both 'protecting my privacy' and 'preventing the loss of my reputation' coefficients had positive signs, however. Perhaps consumers do not consider the behaviour as risky. It is difficult to explain how using 'remember by password' would have an effect on 'reducing my online visibility'. While the p values suggested support for Hypothesis HT2, the direction of the influence did not. Only one of the specific behavioural beliefs, 'websites are easier to use' had a significant path to attitude, providing some support for Hypothesis HT1. None of the general control beliefs had significant paths to PBC, so Hypothesis HT7 was unsupported. Only one of the specific control beliefs 'does not always work' had a significant path to PBC, providing some support for Hypothesis HT6.

As in many of the other behaviours, PBC did not contribute in a substantial way to the model. Its R squared is low at 0.049 and its influence on intention is not significant. Furthermore, some of the beliefs that might be expected to contribute to the model did not. Evidently, "If I wanted to, I could use 'remember my password'" and "For me to use 'remember my password' is easy" tap into somewhat different ideas, since splitting the two indicators that make up PBC and directing them separately to intention increased the path coefficients to significant levels. Neither were significant moderators to the path between intention and behaviour. More of the control beliefs become significant as influences on the two control items.

Figure 31 and Table 39 display the improved model that implements these changes. The R squared of intention went from 0.660 to 0.706. APC increased from 0.276 ($p<0.001$) to 0.304 ($p<0.001$) and ARS increased from 0.213 ($p<0.001$) to 0.292 ($p<0.001$).

As in the other risky behaviours, the concept of perceived behavioural control is not a strong factor in predicting behaviour. Risky behaviours, as a group, are designed to be easy to use and save time, making individual control less of an issue. Of interest, however, are the beliefs that underlie what ultimately becomes behaviour. Saving time, shared computers, and the perception that the 'remember my password' does not always work all play significant parts in predicting this behaviour.

The risky behaviours as a group may be considered shortcuts that save time at the expense of increased risk. They are by nature easy to use and it is therefore not surprising that control issues did not play a large role, as was demonstrated in the analysis of the full sample.

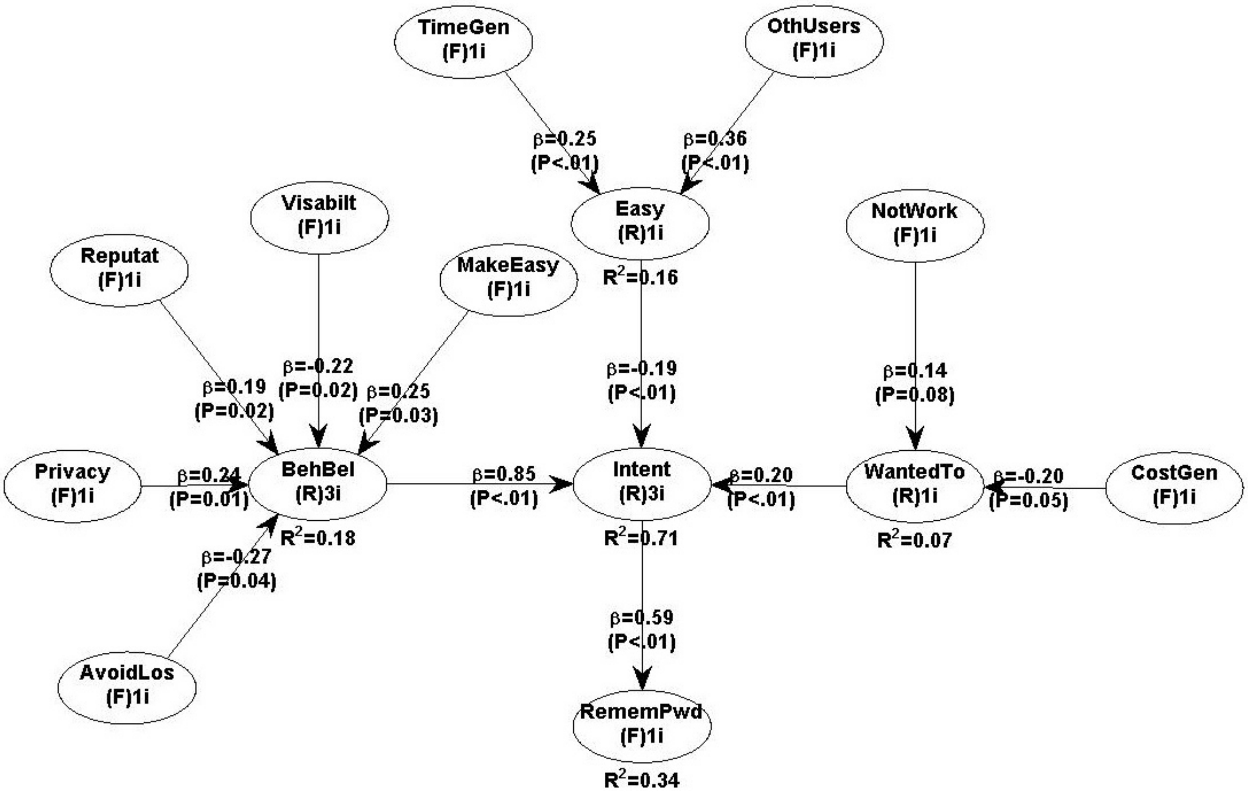


Figure 31 - Improved RememPwd Model

Table 39 - Parameter Estimates for Improved RememPwd Model

RememPwd I select 'remember my card number' or 'remember my password' for online log-ins

Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	WantedTo	Easy
Intent	Intend to use 'remember my password'	0.586				
BehBel	Attitude to using 'remember my password'		0.850			
WantedTo	If I wanted to, I could use 'remember my password'		0.204			
Easy	For me to use 'remember my password' is easy		-0.188			
AvoidLos	Avoiding financial loss (g)			-0.268		
Privacy	Protecting my privacy (g)			0.240		
Reputat	Preventing the loss of my reputation (g)			0.193		
Visabilt	Reducing my online visibility (g)			-0.217		
MakeEasy	Web sites are easier to use			0.252		
CostGen	Costs a lot (g)				-0.200	
NotWork	Does not always work				0.143	
TimeGen	Takes a lot of time (g)					0.251
OthUser	Less secure if other people use my computer					0.364

P Values

Variable	Description	Behaviour	Intention	Attitude	WantedTo	Easy
Intent	Intend to use 'remember my password'	<0.001				
BehBel	Attitude to using 'remember my password'		<0.001			
WantedTo	If I wanted to, I could use 'remember my password'		<0.001			
Easy	For me to use 'remember my password' is easy		0.003			
AvoidLos	Avoiding financial loss (g)			0.043		
Privacy	Protecting my privacy (g)			0.014		
Reputat	Preventing the loss of my reputation (g)			0.025		
Visabilt	Reducing my online visibility (g)			0.020		
MakeEasy	Web sites are easier to use			0.029		
CostGen	Costs a lot (g)				0.050	
NotWork	Does not always work				0.080	
TimeGen	Takes a lot of time (g)					0.004
OthUser	Less secure if other people use my computer					<0.001

Effect Size

Variable	Description	Behaviour	Intention	Attitude	WantedTo	Easy
Intent	Intend to use 'remember my password'	0.344				
BehBel	Attitude to using 'remember my password'		0.691			
WantedTo	If I wanted to, I could use 'remember my password'		0.089			
Easy	For me to use 'remember my password' is easy		0.074			
AvoidLos	Avoiding financial loss (g)			0.061		
Privacy	Protecting my privacy (g)			0.017		
Reputat	Preventing the loss of my reputation (g)			0.031		
Visabilt	Reducing my online visibility (g)			0.026		
MakeEasy	Web sites are easier to use			0.042		
CostGen	Costs a lot (g)				0.045	
NotWork	Does not always work				0.025	
TimeGen	Takes a lot of time (g)					0.046
OthUser	Less secure if other people use my computer					0.116

	Behaviour	Intention	Attitude	WantedTo	Easy
R Squared	0.344	0.706	0.178	0.070	0.162

7.9 Phase 2 Sub-samples - Summary Discussion of TPB with Beliefs

Table 40 shows a summary of support for the TPB hypotheses for all of the sub-samples. In none of the eight analysis groups were all of the hypotheses supported. All of the hypotheses, however, were supported to at least a limited extent in at least one of the analysis groups. Attitude always affected intention and intention always affected behaviour. Subjective norm rarely affected intention and when it did, the sign was reversed. Perceived behavioural control influenced intention for three of the eight analysis groups but had a very limited effect as a moderator of the intention to behaviour path. Behavioural beliefs of some kind, either general identity theft or specific to the behaviour, always had some influence on attitude but control beliefs, general or specific, did not always affect PBC.

PBC does not appear to be as useful as a concept for identity theft behaviours as it does in other contexts. The concept is directed at whether the individual can perform the behaviour, whereas the control issues identified in the preliminary qualitative survey are often more like circumstances where the individual might want to perform the behaviour. The ability to perform is evident in items like 'If I wanted to, I could perform the behaviour' and 'Whether I perform the behaviour is up to me'. The conditions that influence whether the individual might want to perform the behaviours are particularly evident in the 'risky' behaviours. For example, when deciding whether to give personal information over the phone, many individuals mentioned that if they made the call, if they knew the identity of the person on the other end of the line or if they knew how the information would be used, all played a part. None of these considerations impact the ability to give personal information over the phone but might affect the inclination to do so. The success of most of the 'improved' models that were proposed relied on removing 'control' beliefs from PBC and applying them directly to either the intention construct or the behaviour measure, or as a moderator between intention and behaviour. Apologists for TPB would argue that these conditions form part of the context of the behaviour and should be part of its consistent description. By failing to incorporate provisions for context in the model, however, TPB forces behaviour to be so narrowly defined as to severely limit the generality of the model. It also requires that all of the contextual factors be known even before a model is defined.

Identity theft prevention and detection behaviours are not a monolithic set of behaviours but rather a collection of individual components, each of which has its own set of underlying beliefs, some of which may be about identity theft in general and others of which may be specific to the behaviour. The significant behavioural and control beliefs from the TPB models are shown in Table 41. On the whole, the behavioural beliefs are about an even mix of general identity theft beliefs and behaviour-specific beliefs. On closer inspection, the two behaviours in the 'monitoring agencies' component (getting an annual credit report and checking the land registry annually) each have only one general identity crime belief and the behaviour-specific beliefs include the belief that the behaviour has no benefit. These observations suggest that some consumers do not associate these behaviours with identity fraud detection.

There were fewer significant control beliefs than behavioural beliefs associated with each of the analysis groups but again the split between general control beliefs and behaviour-specific control beliefs was about even. There were few significant control beliefs about the three 'risky' behaviours. This might be expected, since all of these behaviours offer expedience at the increased risk of identity theft. Significant barriers to performing the behaviours would defeat their purpose.

Table 40 - Summary of TPB Hypothesis Support

		Credit	Land	Monitor	Physical	Password	Click	Info over	Remember
	TPB Hypothesis	Report	Registry	Accounts	Security	Security	Link	Phone	Password
HT1	An individual’s beliefs specific to a behavioural component positively affects attitudes toward that behavioural component.	X	X		X	x	x	X	X
HT2	An individual’s beliefs about identity theft in general influence attitudes toward all behavioural components.	x		X	X	X	x	x	x
HT3	An individual’s attitudes toward a behaviour component positively affect the intention to perform the component behaviours.	X	X	x	X	X	X	X	X
HT4	An individual’s normative beliefs about identity theft positively affect the individual’s subjective norm.	na	na	na	na	na	na	X	na
HT5	An individual’s subjective norm positively influences the intention to perform identity theft prevention and detection behaviours.								
HT6	An individual’s control beliefs specific to a behavioural component positively affect perceived behavioural control toward that behavioural component.	X	X	X	X				x
HT7	An individual’s control beliefs about identity theft in general influence perceived behavioural control toward all behavioural components.	X		x	x	X		x	
HT8	An individual’s perceived behavioural control of a given behavioural component positively affects the intention to perform component behaviours.	x		X		X			
HT9	An individual’s intention to perform component behaviours positively affects the actual performance of the component behaviours.	X	X	X	X	X	X	X	X
HT10	An individual’s perceived behavioural control of a specific behavioural component moderates the influence of the intention to perform component behaviours on the actual performance of the component behaviours.				x				x

X - supported

x - supported with reservations (p value is greater than 0.05 but less than 0.10 or only a single belief is significant)

na - normative beliefs were not examined if subjective norm had no significant influence on intent

Table 41 - Significant Beliefs for 'Orthodox' TPB Models

	Behavioural	**Control**
Credit Report	Correct mistakes	[#]Costs a lot
	[#]Avoid financial loss	[#]Requires a lot of knowledge
	Information will be stolen	Can easily find how
	Detect unauthorized use	Takes too much time
	Get no benefit	
Land Registry*	Detect any unauthorized mortgage	Costly
	Source of information to thieves	
	Get no benefit	
	Only needed when buying or selling	
	[#]Avoid financial loss	
Monitoring Accounts	[#]Protect my privacy	Takes too much time
	[#]Prevent the loss of reputation	Uncomplicated process
	[#]Avoid financial loss	[#]Requires a lot of knowledge
Physical Security*	[#]Protect my privacy	Takes too much time
	[#]My identity info is secure	[#]Takes a lot of time
	[#]Prevent the loss of reputation	Requires a secure location
	[#]Avoid the hassle of fraud	Requires a shredder
Password Security	Reduce the risk of identity crime	[#]Costs a lot
	[#]Avoid financial loss	[#]Requires diligence
	Online access will be slower	[#]Requires a lot of knowledge
	Will be the victim of identity crime[+]	
Click on Link*	[#]Avoid financial loss	
	[#]Avoid the hassle of fraud	
	Will be the victim of malware	
	Get information tailored to me	
	[#]Stop criminal activity	
Give Info over Phone*	[#]Reduce my online visibility	[#]Requires a lot of knowledge
	Get a good deal	[#]Requires diligence
	[#]Prevent loss of reputation	
Use 'Remember'*	[#]Protect my privacy	Does not always work
	[#]Reduce my online visibility	
	[#]Prevent the loss of reputation	
	Web sites are easier to use	
	[#]Avoid financial loss	

* PBC not significant influence on intention

[+] Reversed scale

[#] General identity theft beliefs - others are specific to the behaviour

7.10 Phase 2 Sub-sample PMT - Results and Discussion

This section applies the sub-sample data to PMT. Eight models were created, one for each of the analysis groups. In addition to the overall severity and vulnerability constructs, the TPB consequences for each behaviour were modeled as severity and the TPB behavioural belief strengths as vulnerability. The TPB subjective norm was modeled as social cost and TPB perceived behavioural control as self-efficacy. PMT response efficacy is built into the TPB consequences and so was not modeled separately. (Since all factors feed into intention in PMT, designating them would not alter the model.) As in TPB, intention is expected to influence behaviour. A generic diagram of the PMT models is shown in Figure 32. The general severity and general vulnerability of identity theft were determined from four and three items respectively in question 9 (PMT questions - page 195) of the general questions section of the survey. All other information was taken from the same sources as the TPB models. Response costs were from the normative question in the general questions and all other items were from the behaviour-specific questions.

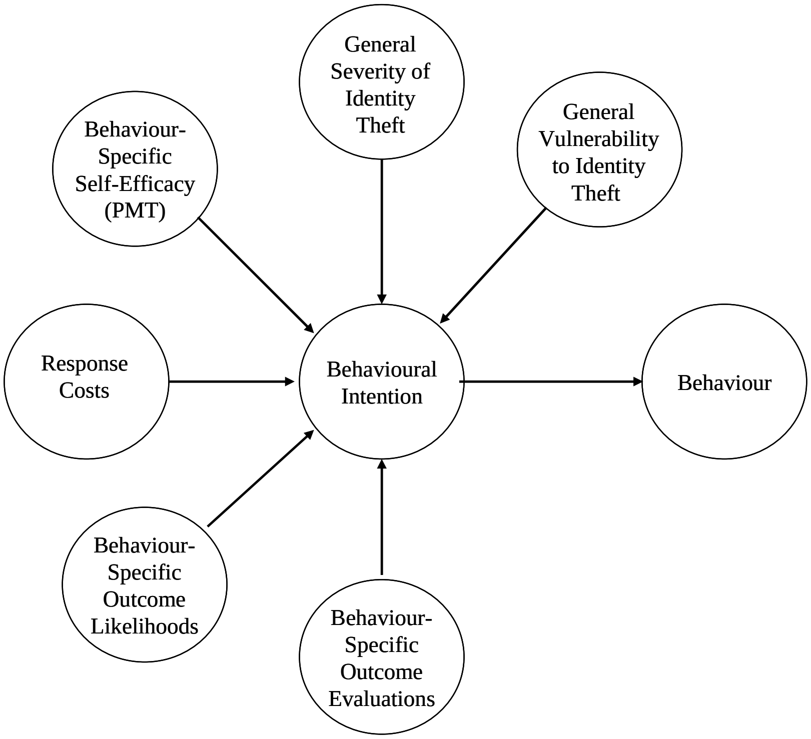

General Severity of Identity Theft
Behaviour-Specific Self-Efficacy (PMT)
General Vulnerability to Identity Theft
Response Costs
Behavioural Intention
Behaviour
Behaviour-Specific Outcome Likelihoods
Behaviour-Specific Outcome Evaluations

Figure 32 - Generic PMT Model

Figure 33 shows the PMT model for the credit report behaviour and Table 42 has the associated parameter estimates. The other behaviours are shown in Appendix Q.

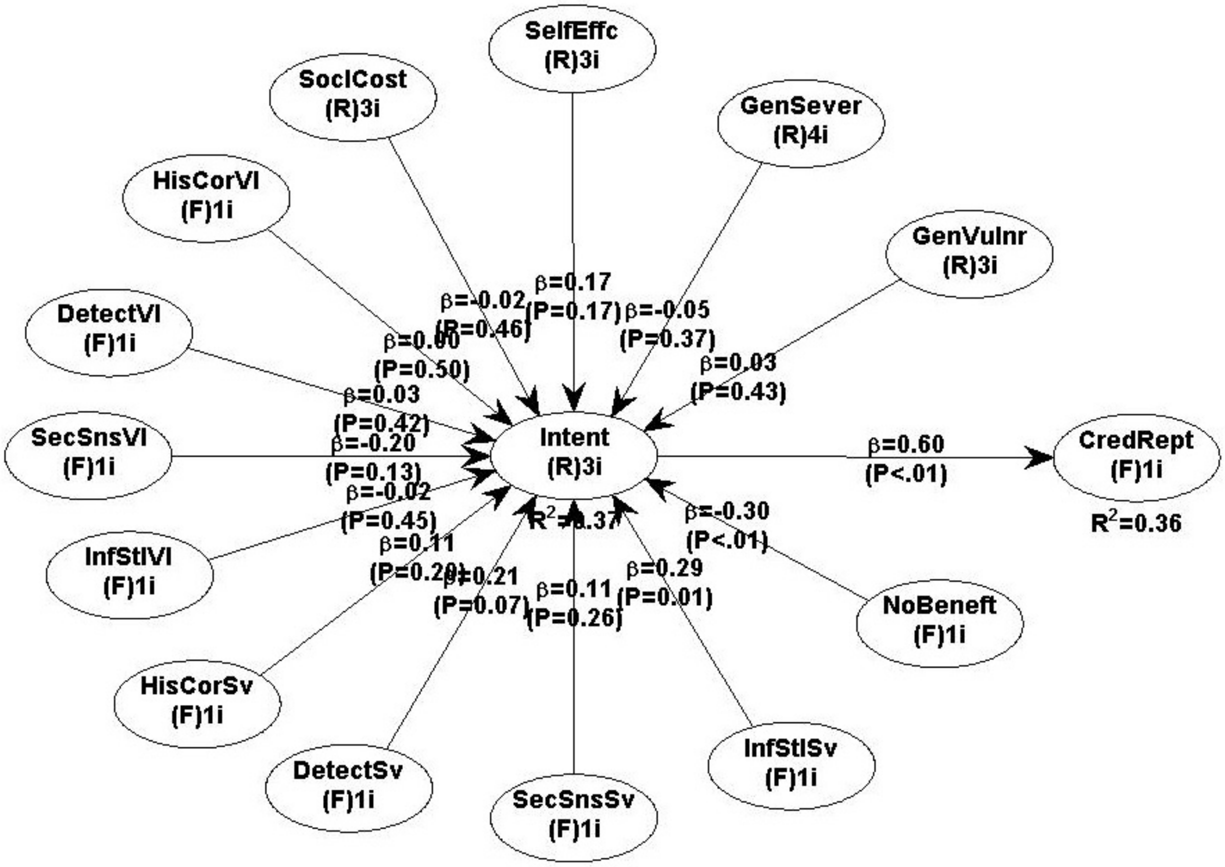


Figure 33 - PMT Model for CredRep ('I request a copy of my credit report at least once a year')

PMT posits that some of the responses to threat may be non-linear and take the form of an inverted U. There is the possibility that as the threat increases beyond a certain point, individuals will undertake 'maladaptive' responses that actually increase a harmful behaviour (Rippetoe and Rogers, 1987). To examine this possibility, the PMT models were rerun using the WarpPLS Warp 2 Regression, which fits using a curve with a single inflection and the curves were then examined to see if the inverted U (or upright U in the case of risky behaviours) materialized.

7.10.1 Phase 2 Sub-sample PMT - Results

For checking credit report behaviour, the effect of intention on behaviour was significant, providing support for Hypothesis HP8 ('An individual's intention to perform the component behaviours will positively affect his or her actual performance of the behaviours'). If the belief that there is no benefit in checking the credit report is classified as a severity, then Hypothesis HP2 ('An individual's assessment of the severity of the consequences of component behaviours affects the intention to engage in component behaviours') was supported by two items. None of the other PMT hypotheses were supported for the credit report behaviour.

Table 42 - Parameter Estimates for PMT CredRep Model

Variable	Description	Path Coefficient	P Value	Effect Size
Intent	Intention	**0.602**	**<0.001**	**0.362**
GenVulnr	General Vulnerability	0.027	0.433	0.005
GenSever	General Severity	-0.053	0.368	0.009
SelfEffc	Self-efficacy	0.172	0.167	0.045
SoclCost	Social Cost	-0.019	0.456	0.002
HisCorVl	History Correction Vulnerability	0.002	0.495	0.000
DetectVl	Detection Vulnerability	0.031	0.419	0.002
SecSnsVl	Secure Sense Vulnerability	-0.196	0.125	0.012
InfStlVl	Information Stolen Vulnerability	-0.016	0.445	0.002
HisCorSv	History Correction Severity	0.110	0.201	0.037
DetectSv	Detection Severity	0.210	0.068	0.088
SecSnsSv	Secure Sense Severity	0.110	0.259	0.043
InfStlSv	Information Stolen Severity	**0.292**	**0.010**	**0.057**
NoBeneft	No Benefit	**-0.303**	**0.008**	**0.113**
	Behaviour R Squared	0.362		
	Intention R Squared	0.370		

Bold indicates significance at the 0.05 level or better

Table 43 is a summary of PMT hypothesis support using similar analysis for each of the eight analysis behavioural groups.

In the PMT models rerun using the WarpPLS Warp 2 Regression, only the 'land registry' behaviour showed an indication of the non-linear response in the expected direction, as shown in Figures 37 and 38.

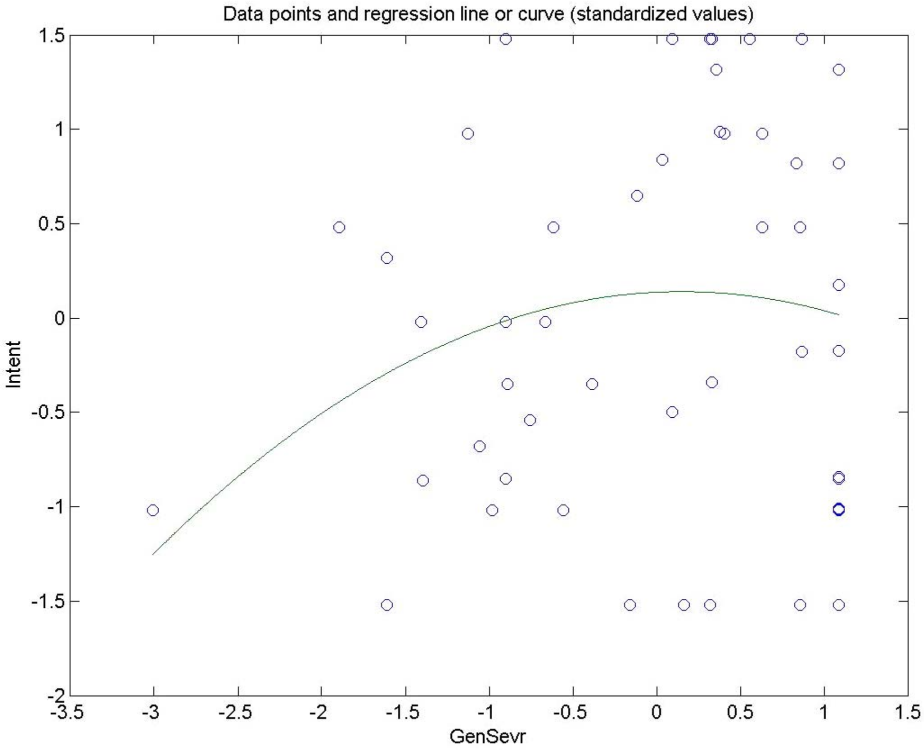


Figure 34 - Response of Intent to General Identity Theft Severity for Land Registry Behaviour

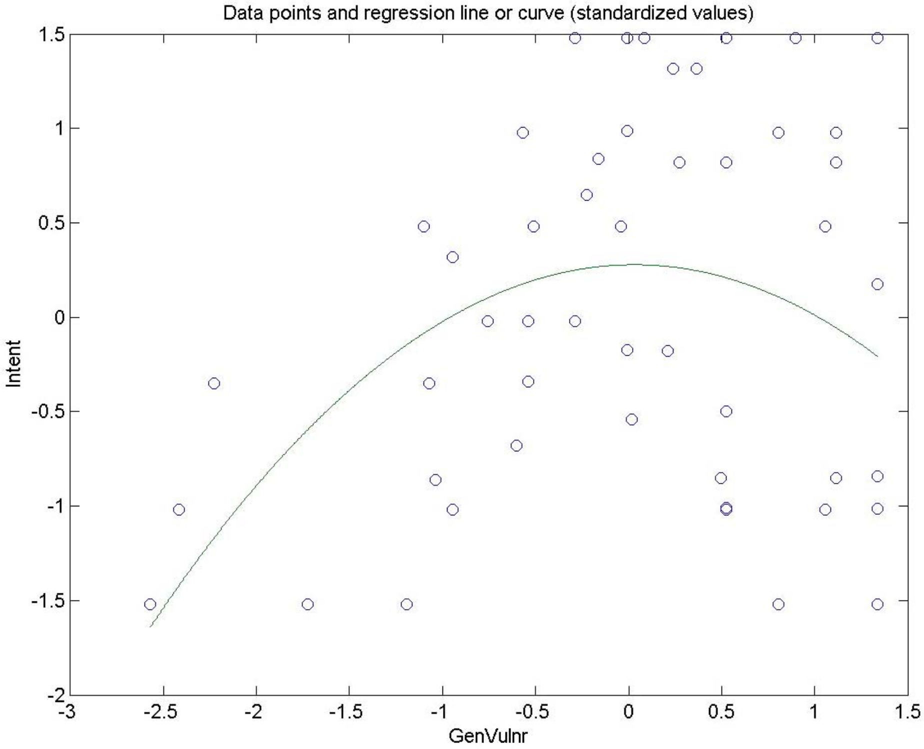


Figure 35 - Response of Intent to General Identity Theft Vulnerability for Land Registry Behaviour

7.10.2 Phase 2 Sub-sample PMT - Discussion

As in the TPB analysis, none of the hypotheses were supported in every behaviour but all but one were supported to some extent in at least one analysis group. The hypothesis that the perception of the severity of the threat of identity theft affects intention (HP1) had no support on any behaviour. The hypothesis that the perception of vulnerability to the threat of identity theft affects intention (HP3) did not fare much better, with solid support in only a single group. The hypotheses that posit that severity and vulnerability to the consequences of individual behaviours affect intention (HP2 and HP4) fare much better, with each finding support on three behaviours. Interestingly, in no analysis group were both HP2 and HP4 supported - it seems to be one or the other. Self-efficacy was supported in six in the eight groups. HP7 (perceived costs affect the intention to perform the behaviour) had virtually no support. This might have been expected, since the only cost explicitly included in the study was social cost. (Other costs were included as consequences, with associated severities and vulnerabilities.) Finally, the influence of intention on behaviour (HP8) was significant for every type of behaviour.

The impact of allowing non-linear responses in the land registry model was overall not positive. The same path coefficients were significant as in the linear model and the APC improved marginally from 0.173 (p=0.042) to 0.198 (p=0.033) but the ARS plummeted from 0.311 (p=0.006) to an insignificant 0.021 (p=13.628).

The significant beliefs for the PMT models are shown in Table 44. Unlike TPB, beliefs about vulnerability to and severity of identity theft in general have almost no influence. Behaviour-specific beliefs dominate.

Table 43 - Summary of PMT Hypothesis Support

	PMT Hypothesis	Credit Report	Land Registry	Monitor Accounts	Physical Security	Password Security	Click Link	Info over Phone	Remember Password
HP1	An individual’s assessment of the severity of identity theft affects the intention to engage in component behaviours.								
HP2	An individual’s assessment of the severity of the consequences of component behaviours affects the intention to engage in component behaviours.	X	X		X				
HP3	An individual’s assessment of his or her vulnerability to identity theft affects the intention to engage in component behaviours.						X		
HP4	An individual’s appraisal of his or her vulnerability to the consequences of component behaviours will affect the intention to engage in component behaviours.					X	X		X
HP5	An individual’s assessment of the response efficacy to counter the threat of identity theft will affect their intention to perform component behaviours.	na	na	na	na	na	na	na	na
HP6	An individual’s appraisal of their ability to perform the behaviour will affect their intention to perform component behaviours.		X	X		X	X	X	X
HP7	An individual’s assessment of the costs of performing the behaviour will affect their intention to perform component behaviours.							x	
HP8	An individual’s intention to perform the component behaviours (protection motivation) will positively affect his or her actual performance of the behaviours.	X	X	X	X	X	X	X	X

X - supported at a p level of 0.05
na - response efficacy is included in the consequences of performing the behaviour and was not separated

Table 44 - Significant Beliefs for PMT Models

Credit Report	No benefit Information stolen severity
Land Registry	Self-efficacy No benefit
Monitor Accounts	Self-efficacy
Physical Security	Have physical record severity Lose personal identity info severity
Password Security	Self-efficacy Being victimized vulnerability
Click on Link	Self-efficacy #General vulnerability Malware victim vulnerability
Give Info Over Phone	Self-efficacy
Use 'Remember'	Self-efficacy Hackers finding password vulnerability

# General identity theft beliefs - all others are specific to the behaviour

7.11 Phase 2 Sub-sample TPB and PMT Comparison

Both TPB and PMT hold that perceptions about a behaviour lead to intentions to perform the behaviour and intentions then lead to actual performance of the behaviour. As implemented in this study, the two main structural differences between the two theories is the inclusion of the attitude and PBC constructs in TPB, and the splitting of severity and vulnerability in PMT. TPB interposes the attitude construct between the perceptions about the behaviour (termed 'beliefs' in TPB) and the intention to perform the behaviour. TPB beliefs are computed by multiplying the perception of the probability that a consequence will occur by the perceived importance of the consequence. PMT uses the same concepts, terming the perceived probability as vulnerability and the importance of the consequence as severity. It does not, however, multiply them together but applies each as a direct effect on intention. A third difference is the moderation of path from intention to behaviour by perceived behavioural control that is part of TPB but not PMT. In this study, that difference was found to have little effect, since only two of the eight analysis groups provided support for the TPB hypothesis at the 0.10 level, with none at the 0.05 level.

A quantitative comparison of the two theories appears in Table 45. The R squared of the intention construct, and the APC and ARS were obtained from the TPB models in Appendix P and the PMT models in Appendix O. The theory with the highest value in each measure for each analysis group is shown in bold in Table 45.

Table 45 - Quantitative Comparison of TPB and PMT

	Intent R squared		APC		ARS	
Analysis Group	TPB	PMT	TPB	PMT	TPB	PMT
Credit Report	**0.706**	0.370	**0.175**	0.153	**0.419**	0.366
Land Registry	**0.613**	0.533	**0.178**	0.173	**0.351**	0.311
Monitor Accounts	**0.741**	0.678	0.149	**0.194**	0.414	**0.461**
Physical Security	**0.626**	0.559	**0.205**	0.185	0.333	**0.388**
Password Security	**0.783**	0.744	0.128	**0.156**	0.386	**0.437**
Click Link	**0.533**	0.306	0.125	**0.166**	**0.223**	0.211
Info over Phone	**0.566**	0.173	0.129	**0.136**	0.234	**0.257**
Remember Password	**0.660**	0.352	**0.172**	0.161	0.349	**0.353**
Weighted Average	**0.651**	0.448	0.157	**0.164**	0.336	**0.345**

Bold - Highest value in each measure for each analysis group

The effect of the inclusion of the attitude construct in TPB is evident in the R squared value for the intention construct. As expected, the attitude toward the behaviour explains a lot of the intention to do it. The high R squared values for intent did not result in higher Average R Squared (ARS), however. PMT had higher ARS values in five of the eight analysis groupings and a slightly larger weighted average. TPB and PMT did equally well on Average Path Coefficient (APC) measures, with each getting the largest value on four of the behaviours but PMT getting a slightly larger weighted average. The imposition of the attitude construct between the behavioural beliefs and intent constructs in TPB generated higher R squared values for the intention construct but lower R squared values for the attitude and other constructs, which resulted in ARS values about the same as PMT.

In a comparison of Tables 36 and 39, other findings surface. The self-efficacy construct in PMT, which, as modeled in this study, is identical to PBC, was significant in five analysis groups in

PMT but only three in TPB. It appears as if the high correlation between the attitude construct in TPB accounted for most of the variance and did not leave much for PBC to explain. The perceptions of vulnerability and severity of identity theft in general were not as good in explaining the variation in intent as the general beliefs in TPB.

Although PMT appears to have a quantitative edge, TPB exposed more of the salient beliefs and the attitude construct in this model explained more of the intention to perform the behaviour. The severity and vulnerability constructs in PMT for identity theft in general were not as effective as the TPB beliefs about identity theft in general. The Achilles' heel of TPB is the rigid specification of the behaviour in action, target, context, and time. By narrowly defining the attendant conditions of the behaviour, TPB severely limits the generality of its models. In the context of identity theft prevention and identity fraud detection behaviours, neither TPB nor PMT explained a large part of the behaviour. The common failing is the gap between intention and behaviour in the application of both theories.

Chapter 8. Phase 2 Qualitative Analysis Results and Discussion

Most of the respondents provided answers to three qualitative items. Some of the respondents abandoned the survey before completion but did provide qualitative input. Since the demographic data were available, their input was included in the qualitative analysis. Some of the respondents included in the quantitative analysis did not provide qualitative responses or just typed 'nonsense' to get to the next question. After these two factors were considered, the qualitative data from 408 respondents were considered. French responses were translated into English before processing.

8.1 Coding

Three questions were posed to elicit qualitative data (page 196 in Appendix D):

1. In what ways do you think you are most vulnerable to identity theft?
2. What do you think are the most important things you can do to prevent identity theft?
3. What do you think are the most important things you can do to detect identity fraud?

Unfortunately, it was clear from the responses that some respondents read the difference between questions 2 and 3 as 'theft' versus 'fraud' and ignored the 'prevent' versus 'detect' aspect. The responses from questions 2 and 3 were processed together and the codings classified into the question for which the response was appropriate. For example, if a response to question 2 was 'checking my credit card statement', it was deemed to be a response to question 3 since checking a credit card statement cannot prevent identity crime but only detect it. Responses were open-coded and then the codes were categorized into code classes. An individual response might generate multiple codings but only a single instance of a given code. For example, no matter how many times a given respondent mentioned monitoring his or her credit cards and/or bank statements in response to question 3, the input was awarded only one code of 'monitor accounts'. The number of codes applied, along with the number of distinct codes for each question, is shown in Table 46.

Table 46 - Codes Applied to Qualitative Data

Question	Unique Codes	Codes Applied
1	34	552
2	46	862
3	10	369
Total	90	1783

Table 47 - Inter-Rater Reliability Measures

Question 1				
Statistic	Kappa[16]	Scott[17]	Gwet[18]	Brennan Prediger[19]
Coefficient	0.817	0.817	0.824	0.824
Standard Error	0.018	0.018	0.017	0.017
95% Lower Conf. Limit	0.781	0.781	0.790	0.790
95% Upper Conf. Limit	0.852	0.852	0.858	0.858
One-Sided P-Value	0.000	0.000	0.000	0.000
Two-Sided P-Value	0.000	0.000	0.000	0.000
Z-Value	45.469	45.435	47.469	47.305
Question 2				
Statistic	Kappa	Scott	Gwet	Brennan Prediger
Coefficient	0.798	0.798	0.809	0.808
Standard Error	0.015	0.015	0.015	0.015
95% Lower Conf. Limit	0.768	0.768	0.780	0.779
95% Upper Conf. Limit	0.828	0.827	0.837	0.837
One-Sided P-Value	0.000	0.000	0.000	0.000
Two-Sided P-Value	0.000	0.000	0.000	0.000
Z-Value	52.718	52.394	55.503	55.269
Question 3				
Statistic	Kappa	Scott	Gwet	Brennan Prediger
Coefficient	0.844	0.844	0.903	0.899
Standard Error	0.025	0.025	0.016	0.017
95% Lower Conf. Limit	0.796	0.796	0.871	0.866
95% Upper Conf. Limit	0.892	0.892	0.935	0.932
One-Sided P-Value	0.000	0.000	0.000	0.000
Two-Sided P-Value	0.000	0.000	0.000	0.000
Z-Value	34.438	34.431	55.557	53.351

[16] Cohen, 1960
[17] Scott, 1955
[18] Gwet, 2008
[19] Brennan and Prediger, 1981

Another researcher independently coded the three questions and the results were categorized into code classes and compared. The results are shown in Table 47. For the most part, inter-rater reliability exceeded 80% which is considered as 'almost perfect' (Landis and Koch, 1977) or 'excellent' (Fleiss, 1981).

8.2 Frequency Analysis

The frequency of the number of times each code was mentioned, along with the higher level code classifications, is in Appendix R (page 266). The high level code classification frequencies for each question response are displayed in Figures 39, 40 and 41. (Note that the percentages do not add to 100% since some respondents mentioned more than one code item.)

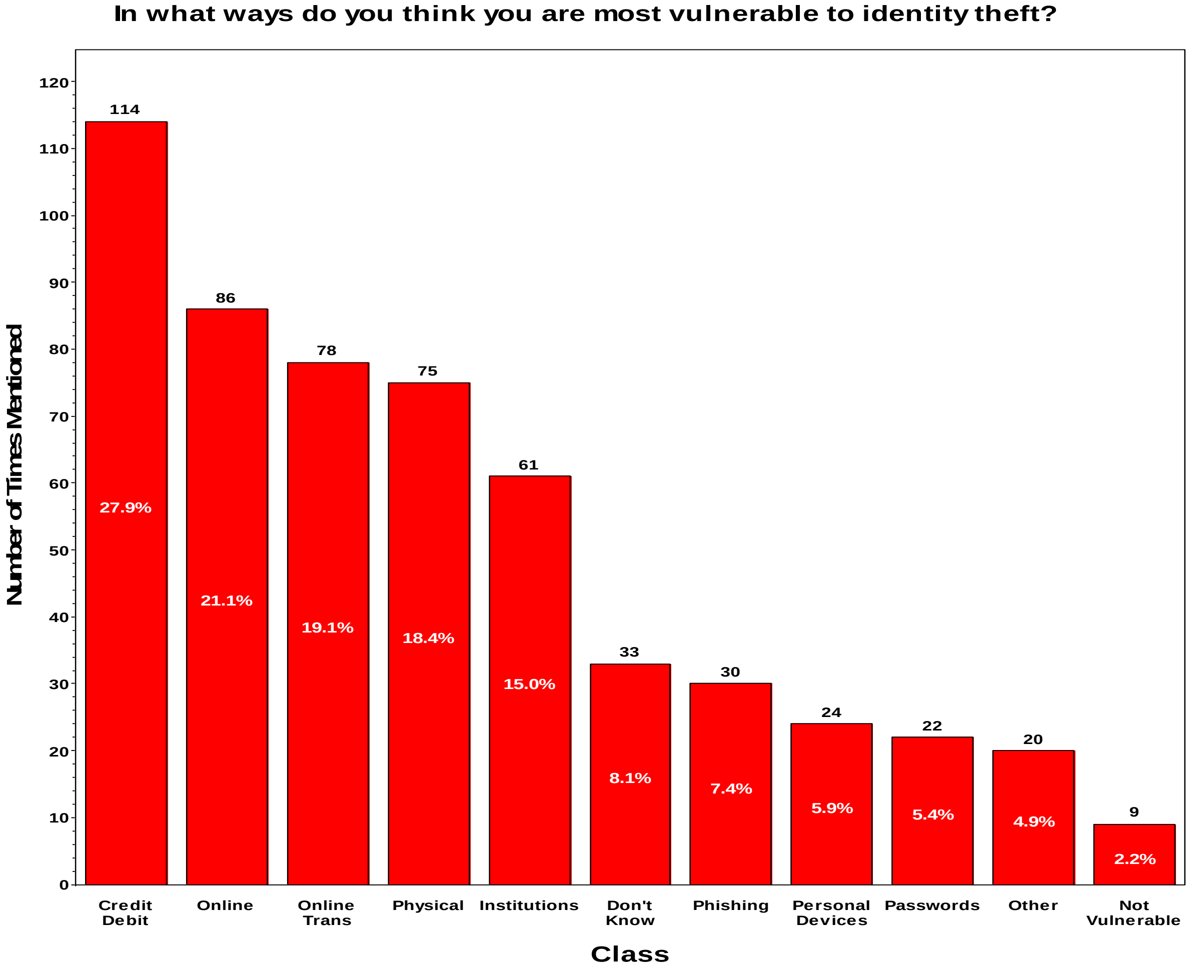


Figure 36 - Responses to Qualitative Question 1

The most mentioned vulnerability was credit and debit cards (including ATMs and card skimming) for over one quarter (28%) of respondents. Generally being online and social media came next with 21% of respondents. About one fifth (19%) were concerned about online transactions including online purchases and sales and online banking. Almost as many (18%) felt vulnerable to physical identity theft (theft of documents such as passports, social insurance

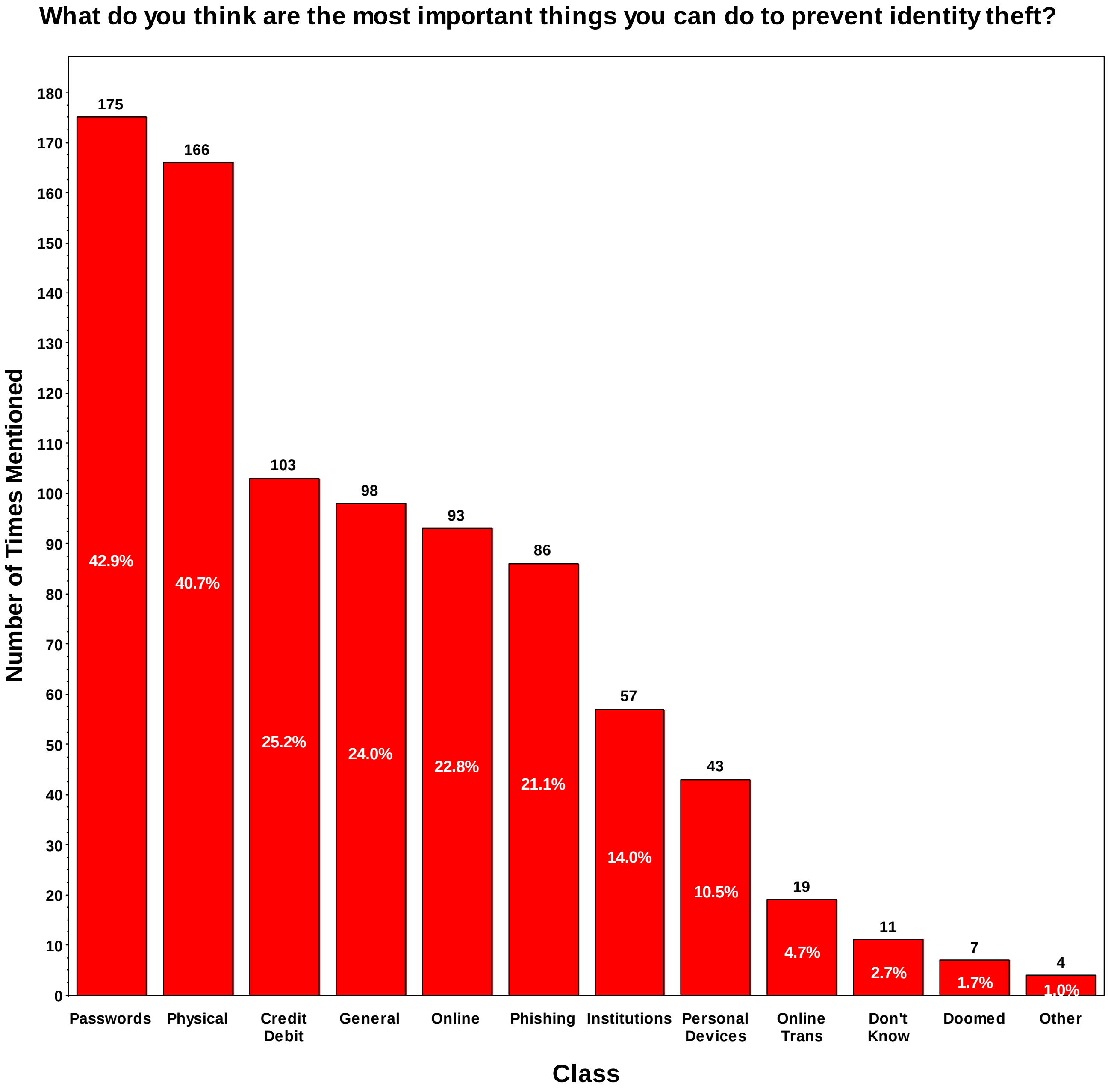


Figure 37 - Responses to Qualitative Question 2

cards, vulnerability of regular mail, and wallets/purses etc.) and 16% felt vulnerable due to data breach and data collection by businesses and public institutions. All the other classes were mentioned by less than 10% of respondents. The largest of these is interesting: 8% did not know in what way they were most vulnerable. A brave 9 respondents (2%) did not feel they were vulnerable.

When it comes to preventing identity theft, two classes figure most prominently: passwords and physical measures, with 43% and 41% respectively. The frequency of password mentions corroborates the high positive attitude and intention scores in the quantitative part of the survey. Physical security attitudes and intention values were also very high (see Appendix K). Rounding out the classes with more than 10% of respondents were credit/debit cards (25%), general caution (24%), online measures such as using secure websites, limiting personal information of social media, and general online caution (23%), resisting 'phishing' attacks (21%), dealing only with known entities and other measures dealing with institutions (14%), and measures to secure personal devices such as deleting cookies, avoiding 'remember my password' and other auto-fill facilities, avoiding 'public' computers and using and keeping up-to-date antivirus software (11%).

There are some discrepancies in the ways consumers perceived vulnerabilities and preventative measures. Passwords were mentioned by only 5% of respondents when asked about vulnerabilities but by 43% when queried about prevention measures. In a similar, although not as dramatic vein, physical security was mentioned as a vulnerability by only 18% of respondents but by 41% when asked about measures to prevent identity theft. 'Phishing' and personal devices did not appear as vulnerabilities but were mentioned by more than 10% of respondents as preventative measures (see Table 48).

One of the sources of the differences was that respondents were simply more forthcoming on the prevention measures question, with 862 codes versus the 552 for the vulnerability question. The other possible explanation is that due to the prevention measures currently undertaken and mentioned in question2, consumers did not feel vulnerable and the issue was not mentioned in question 1. For example, consumers may have a daily taste of 'phishing' attacks but because they believe they can easily recognize and delete them, they do not feel vulnerable.

Table 48 - Summary of Responses to Qualitative Questions 1 and 2

Code Class	Vulnerability		Preventative Measures	
	#	%	#	%
Credit/Debit	114	27.9	103	25.2
Online	86	21.1	93	22.8
Online trans	78	19.1	19	4.7
Physical	75	18.4	166	40.7
Institutions	61	15.0	57	14.0
Don't know	33	8.1	11	2.7
Passwords	22	5.4	175	42.9
General			98	24.0
Phishing			86	21.1
Personal devices			43	10.5

The overwhelming response to the question of the detection of identity fraud was the monitoring of bank accounts and credit cards, with 57% mentioning that issue. The response corroborates the very positive attitude and intention scores on the quantitative portion of the survey. 15% mentioned checking their credit report. 10% said they did not know. Note that this was not a case of blank responses (which were left uncoded) but an actual expression of lack of knowledge.

In physics, the 'observer effect' states that by measuring a phenomenon, you irretrievably alter it (this is due to the fact that energy must be either added or extracted to effect a measurement). Some of that sort of issue seems to have occurred in this survey. One of the respondents to the third (detection) question wrote '...and now I know to get a credit report and a registry office check once a year'. Apparently the information that was imparted just by asking the early survey questions had an effect on the responses to the later ones. The extent of this 'observer effect' is unknown.

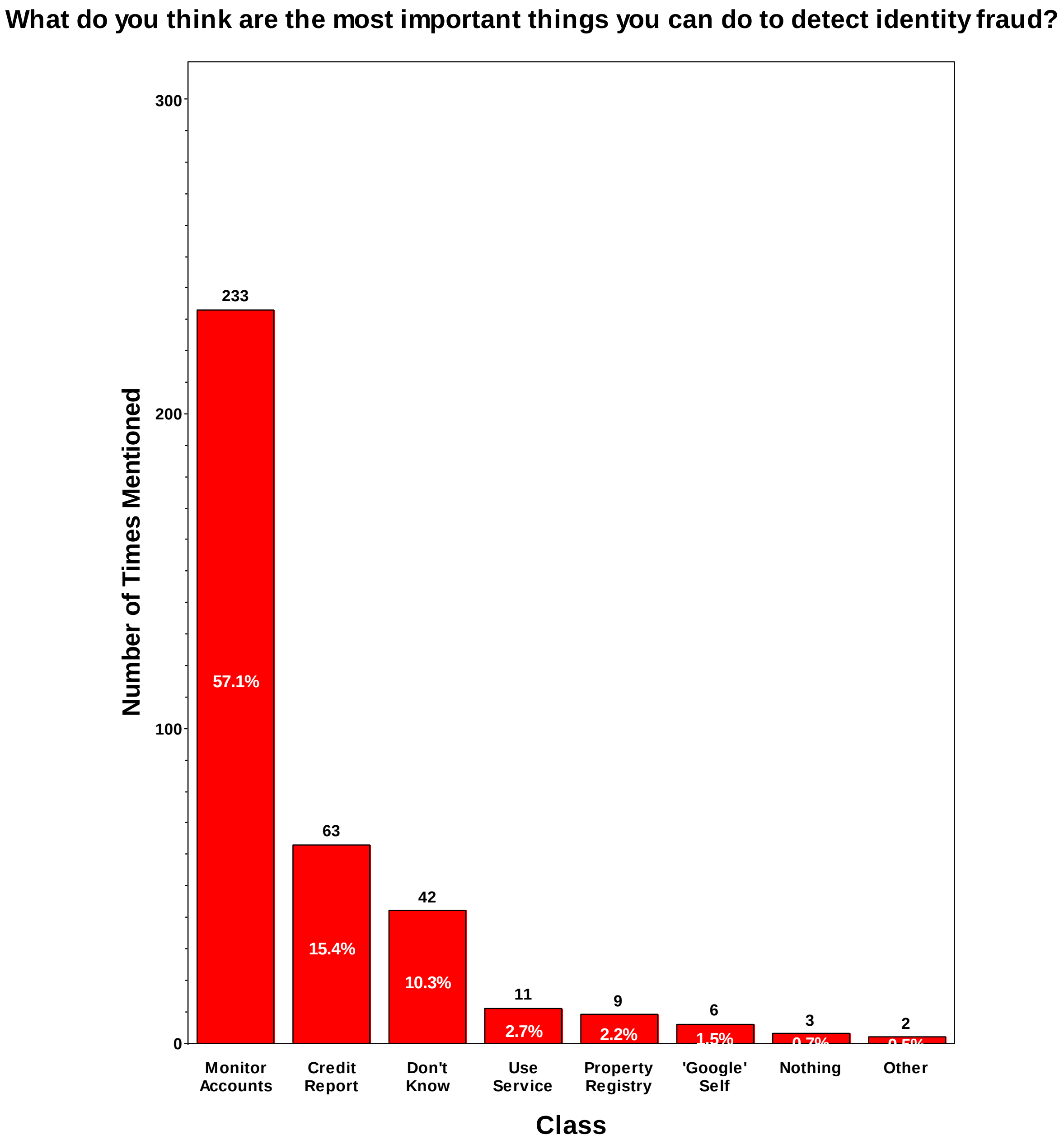


Figure 38 - Reponses to Qualitative Question 3

8.3 Logistic Regression

While the frequency analysis is interesting, it might be illuminating to delve into the circumstances behind the mention of each class of code. Since the criterion variable is dichotomous (either the class code is mentioned or not), a simultaneous logistic regression was used to model whether a respondent mentioned a code classification. The predictor variables, obtained largely from the screening and demographic items, were the number of bank accounts, number of credit cards, age, language, gender, whether respondents had ever been the victim of credit card fraud, had ever been a victim of other identity fraud, and home ownership. For age, the midpoint of the age range was used. For language, English was coded as 0 and French as 1. For gender, males were coded as 0 and females as 1. For credit card fraud and other identity fraud, 1 was coded if respondents had reported ever being a victim and 0 if they had not. Home owners were coded as 1 and others coded as 0. To provide some statistical power, only classes with mentions by more than 10% of the respondents were analyzed. The overall significance measures are shown in Table 49 and the maximum likelihood estimates are shown in Appendix S.

All of the test measures agreed on which models were significant. For the vulnerability question, the models for mentions of 'online transactions' and 'out of personal control' were significant at the 0.05 level and both were significant at the 0.01 level, with the exception of the Wald test for 'out of personal control'. For the prevention question, only the 'phishing' model was significant at the 0.05 level. All of the detection models, 'monitoring accounts', 'checking credit report' and 'I don't know', were significant at the 0.05 level, with 'monitoring accounts significant' at the 0.01 level for all measures and 'checking credit report' significant at the same level for two of the three measures.

The parameter estimates for the significant models for the vulnerability question (question 1) are shown in Table 50. Only significant predictor variables are shown. Controlling for all the other predictor variables, females were 1.8 times as likely as males (p=.0358) and English speakers were 4.2 times a likely as French speakers (p=.0004) to mention online transactions. Likelihood of mentioning online transactions decreases with age, with the probability of .75 for each 10 years of increased age (p=.0038).

Table 49 - Logistic Regression Testing Global Null Hypothesis for Qualitative Data

1. In what ways do you think you are most vulnerable to identity theft?

		Likelihood Ratio		Score		Wald	
Code Class	DF	Chi-Square	Pr > ChiSq	Chi-Square	Pr > ChiSq	Chi-Square	Pr > ChiSq
Credit/Debit Cards	8	11.9017	0.1556	12.1574	0.1443	11.7555	0.1624
Online	8	12.3228	0.1374	12.2393	0.1408	11.8182	0.1595
Physical	8	6.6131	0.5789	6.6620	0.5735	6.5122	0.5901
Online Transactions	8	**28.0205**	**0.0005**	**25.2408**	**0.0014**	**23.0729**	**0.0033**
Out of Personal Control	8	**21.5466**	**0.0058**	**21.0818**	**0.0069**	**19.7358**	**0.0114**

2. What do you think are the most important things you can do to prevent identity theft?

		Likelihood Ratio		Score		Wald	
Code Class	DF	Chi-Square	Pr > ChiSq	Chi-Square	Pr > ChiSq	Chi-Square	Pr > ChiSq
Credit/Debit Cards	8	7.7052	0.4628	7.9169	0.4416	7.7032	0.463
Online	8	12.1501	0.1446	11.9556	0.1532	11.5727	0.1713
Physical	8	11.2858	0.186	11.2143	0.1899	10.918	0.2064
Out of Personal Control	8	5.2867	0.7265	5.1877	0.7373	5.1051	0.7463
Phishing	8	**19.6127**	**0.0119**	**19.6359**	**0.0118**	**18.4608**	**0.018**
Passwords	8	15.4779	0.0505	15.0649	0.0579	14.5734	0.068
General Caution	8	10.218	0.2501	9.7817	0.2807	9.5223	0.3002

3. What do you think are the most important things you can do to detect identity fraud?

		Likelihood Ratio		Score		Wald	
Code Class	DF	Chi-Square	Pr > ChiSq	Chi-Square	Pr > ChiSq	Chi-Square	Pr > ChiSq
Monitor Accounts	8	**24.6451**	**0.0018**	**24.1567**	**0.0022**	**22.8901**	**0.0035**
Check Credit Report	8	**24.5484**	**0.0019**	**21.3863**	**0.0062**	**18.6693**	**0.0167**
Don't Know	8	**17.5177**	**0.0251**	**17.2046**	**0.028**	**15.9339**	**0.0433**

Bold indicates significance at the 0.05 level

Concern about lack of personal control decreased with the number of credit cards the individual owned and increased with age. Respondents were .73 times (p=.0185) as likely to mention the topic for each additional card owned and 1.26 times as likely (p=.0186) for each additional decade of age. Credit card victims were 1.9 times as likely as non-victims (p=.0437) and home owners were .472 times as likely as home non home owners (p=.0139) to mention lack of personal control.

Table 50 - Parameter Estimates for Significant Vulnerability Models

Analysis of Maximum Likelihood Estimates							
Parameter	DF	Estimate	Standard Error	Chi-Square	Pr > ChiSq	Odds Ratio	Label
Online Transactions							
AGE	1	-0.0297	0.0102	8.3924	0.0038	0.971	Age
LANGUAGE	1	-1.4361	0.4021	12.7548	0.0004	0.238	Language
SEX	1	0.5880	0.2801	4.4081	0.0358	1.800	Gender
Out of Personal Control							
N_CARDS	1	-0.3148	0.1336	5.5528	0.0185	0.730	# Credit Cards
AGE	1	0.0237	0.0101	5.5429	0.0186	1.024	Age
CARDVICT	1	0.6403	0.3175	4.0668	0.0437	1.897	Card Victim
OWNHOME	1	-0.7499	0.3047	6.0567	0.0139	0.472	Home Owner

The parameter estimates for the significant models for the prevention question are shown in Table 51. Only significant predictor variables are shown. Older individuals were more likely to mention 'phishing' precautions as a measure to prevent identity theft, controlling for all the other predictor variables. Respondents were 1.37 times as likely to mention the issue for each additional decade of age (p=.0006).

Table 51 - Parameter Estimates for Significant Prevention Models

Analysis of Maximum Likelihood Estimates							
Parameter	DF	Estimate	Standard Error	Chi-Square	Pr > ChiSq	Odds Ratio	Label
Phishing							
AGE	1	0.0313	0.00911	11.7890	0.0006	1.032	Age

The parameter estimates for the models for the detection question are shown in Table 52. Only significant predictor variables are shown. English speakers were almost twice as likely (1.98, p=.0036) as French speakers to mention monitoring bank accounts and/or credit cards as a method of detecting identity fraud, controlling for all the other predictor variables. Females were 1.8 times as likely as males to mention the topic. Language again emerged as a predictor in the likelihood of mentioning checking credit reports, with English speakers more than five times (5.26, p=.0006) as likely as French speakers to mention it. French speakers were exactly twice as likely as English speakers (p=.0473) to profess to not knowing how to detect identity fraud. Credit card victims were 2.17 times as likely as non-victims (p=.0297) to claim to not know how to detect identity fraud. (The use of 'don't know' is likely genuine, rather than a quick way to get through the questions, since only 6 out of the 408 respondents used the 'don't know' response for all three qualitative questions.)

Table 52 - Parameter Estimates for Significant Detection Models

Analysis of Maximum Likelihood Estimates							
Parameter	DF	Estimate	Standard Error	Chi-Square	Pr > ChiSq	Odds Ratio	Label
Monitor Accounts							
LANGUAGE	1	-0.6825	0.2343	8.4880	0.0036	0.505	Language
SEX	1	0.6051	0.2091	8.3753	0.0038	1.832	Gender
Check Credit Report							
LANGUAGE	1	-1.6621	0.4873	11.6320	0.0006	0.190	Language
Don't Know							
LANGUAGE	1	0.6931	0.3495	3.9332	0.0473	2.000	Language
CARDVICT	1	0.7730	0.3555	4.7286	0.0297	2.166	Card Victim

There are clearly some cultural differences here. French speakers are less likely to be concerned about online transactions, less likely to note monitoring accounts and checking their credit reports as methods of detecting identity fraud, and twice as likely to admit to not knowing how to detect identity fraud. Since French speakers are generally less likely to mention a particular issue, this could be just a difference in the participation; that is, English speakers may make more substantial comments and therefore are more likely to mention a given one. To test this hypothesis, descriptive statistics were obtained for the number of codes for each qualitative question by language. Table 53 displays the results.

Table 53 - Descriptive Statistics for Number of Codes by Language

Question	English			French		
	N	Max	Mean	N	Max	Mean
Vulnerability	290	6	1.45	107	3	1.23
Prevention	290	8	2.25	106	6	1.97
Detection	228	3	1.28	71	2	1.08
Weighted Average			1.69			1.47

The numbers of codes for French responses were indeed consistently smaller for all three questions, calling into doubt the linguistic differences in the logistic regression analysis. The odds ratios (4.20, 1.98, 5.26 and 2.00), however, are quite large and unlikely to be an artefact of the percentage differences in response.

There were also some significant differences based on age, with older respondents less likely to be concerned about online transactions, more likely to be concerned about the vulnerability of institutions to identity theft, and more likely to mention 'phishing' as an identity theft protection measure. These differences might also be caused by different response volumes. The correlation between age and number of codes is shown in Table 54. The 'out of personal control' logistic regression effect might be a response volume effect, since there is a significant correlation between the number of codes and age for the vulnerability question. The 'institution' concern cannot be a response volume effect, since the sign of the logistic regression coefficients is different from that of the correlation. The correlation coefficient for the prevention question is not significant suggesting that the relation between age and 'phishing' in the logistic regression is real.

Table 54 - Correlation between Age and Number of Codes

Question	N	Correlation Coefficient	P-Value
Vulnerability	397	0.101	0.044
Prevention	396	0.088	0.079
Detection	299	0.077	0.182

There were also differences between males and females, with females more likely to be concerned about online transactions and more likely to mention monitoring accounts and credit cards as a method of detecting identity fraud. These differences could be a response volume effect but it is unlikely given the slight differences in response, as indicated in Table 55.

Table 55 - Descriptive Statistics for Number of Codes by Gender

Question	Female			Male		
	N	Max	Mean	N	Max	Mean
Vulnerability	219	5	1.42	178	6	1.36
Prevention	219	7	2.29	177	8	2.04
Detection	173	3	1.21	126	3	1.26
Weighted Average			1.67			1.58

All of the other significant logistic regression coefficients are associated with only a single prediction variable, with odds ratios large enough that they are unlikely to be artefacts of response volume.

These finding are of practical interest. They suggest that there are demographic factors that are significantly linked to consumer beliefs about identity theft and fraud. These factors need to be incorporated into any plans to raise public awareness of identity theft and fraud.

8.4 Triangulation with Quantitative Results

Some of the qualitative code classes align reasonably well with some of the eight quantitative analysis groupings. To triangulate the logistic regression results from the qualitative data, linear regressions were performed on the corresponding quantitative data. The attitude construct is the most appropriate analogous measure to the qualitative results, since the qualitative items elicit perceptions.

To link the qualitative data to the quantitative data, those concerned about online transactions from the qualitative results might be likely to have a negative attitude toward using 'remember my password'. Those concerned about 'phishing' might be likely to have a negative attitude toward clicking on a link in an e-mail. The most straightforward connections are those between mentioning monitoring accounts and credit reports as detection measures in the qualitative section and the attitudes toward monitoring accounts and checking credit reports in the quantitative section. Linear regressions were performed using the significant demographic variables from the logistic regression as predictors of the corresponding attitude construct from the quantitative data. The results are shown in Table 56.

Table 56 - Linear Regression Parameters

Qualitative Class	Quantitative Attitude	Demographic Variable	Parameter	p Value
Online Transactions	Remember my Password	Age Language Gender	-0.00744 -0.72660 -0.02172	0.0571 0.0031 0.9183
Phishing	Click on link in e-mail	Age	-0.01152	0.0570
Monitor Accounts	Monitor Accounts	Language Gender	-0.02746 0.13495	0.8117 0.1797
Check Credit Report	Check credit report	Language	-0.64848	0.0023

As in the logistic regression, language was a significant predictor for attitude toward using 'remember my password' and age was marginally significant, while gender was not significant. Age was a marginally significant predictor of the attitude toward clicking on a link in an e-mail but the sign was opposite of that in the logistic regression on mentions of 'phishing'. In the most straightforward of the relationships between the qualitative and quantitative, the results were mixed. Language and gender, which were significant at the 0.01 level in the logistic regression for mentions of monitoring accounts, were not at all significant as predictors of the attitude toward monitoring accounts. Language was a significant predictor of the attitude toward checking one's credit report. All of the signs for the significant parameters, except as noted, agreed with the logistic regression.

Overall the linear regressions of the quantitative data provide some corroboration of the qualitative data. The most unexpected result was the insignificance of the predictors of the monitoring accounts behaviour, since it had the most direct correspondence in the two sets of data. This may be due to the extremely skewed distribution of positive attitude toward monitoring accounts (see Appendix K). Monitoring accounts seems to be a 'motherhood' issue that just about everyone has a positive attitude toward. There is little variation to be explained in this measure.

Chapter 9. Phase 2 Credit Cards as Identity Theft - Results and Discussion

As noted in Chapter 2 (Background), there has been on-going discussion as to whether credit card fraud should be considered identity theft and fraud. Two items were incorporated into the survey to elicit the perceptions of consumers as to whether they considered credit card fraud as distinct: I05 ('I worry less about credit card fraud than other identity fraud') and I10 ('Credit card fraud is much less serious than other identity fraud').

9.1 Phase 2 Credit Cards as Identity Theft Results

The results of items I05 and I10 are in Figures 42 and 43.

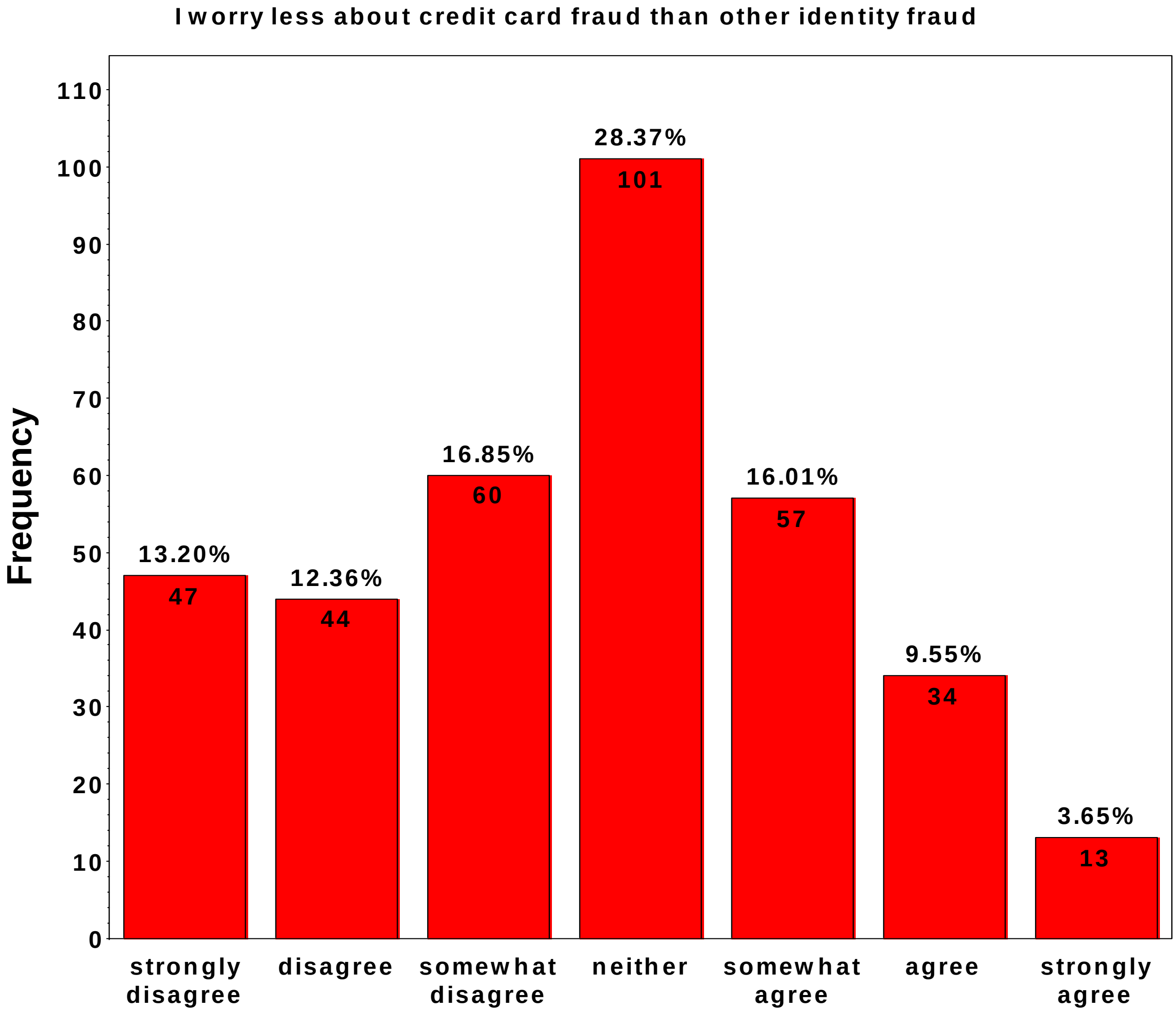


Figure 39 - Responses to Question I05

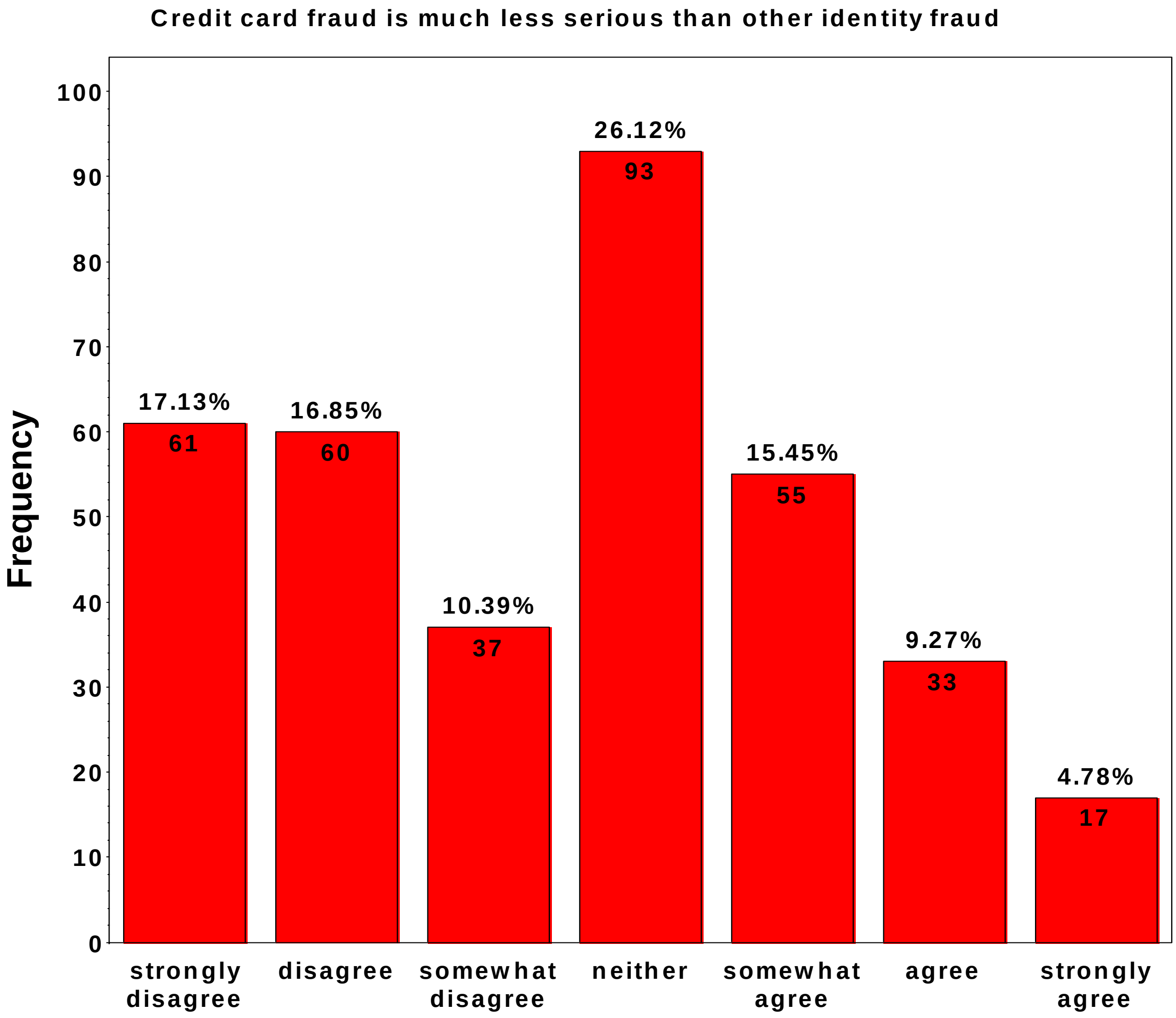


Figure 40 - Responses to Question I10

9.2 Phase 2 Credit Cards as Identity Theft Discussion

It seems that consumers as a whole are convinced that credit card fraud is as serious and causes as much worry as other identity fraud. Only 13.2% agree or strongly agree that they worry less about credit card fraud, whereas 25.6% disagree or strongly disagree. The largest group (28.4%) considers credit card fraud and other identity fraud as equally worrisome. Only 14.1% agree or strongly agree that credit card fraud is much less serious than other identity fraud, whereas 34.0% disagree or strongly disagree. Again, the largest group (26.1%) finds credit card fraud and other identity fraud equally serious.

Chapter 10. Conclusion

10.1 Summary of Findings

This section revisits the research questions raised in Chapter 3 and provides a summary of findings.

1) What are the salient consumer beliefs about the consequences and outcomes of identity theft prevention and identity fraud detection behaviours that influence attitudes toward behaviours and, in turn, intentions to perform the behaviours?

This research question aligns with Hypothesis HT1 (behaviour-specific beliefs affect attitude) which was supported in five behavioural groups and marginally supported in a further two (see table 41 for details). Beliefs about specific behaviours or types of behaviour seem to have had as much or more influence as beliefs about identity theft behaviours in general and each analysis behavioural group had its own distinctiveness.

The 'getting a credit report' and 'checking the land registry office' behaviours had some beliefs of particular interest. Both had significant beliefs that these behaviours have no benefit and that if credit reports or land registry reports are obtained, they may fall into the hands of identity thieves. Another significant belief was that checking the land registry office is needed only when buying or selling property.

Monitoring accounts (bank accounts and credit cards) seems to be a behaviour that is particularly associated with identity theft detection in the belief systems of consumers. All of the significant beliefs were about identity theft in general and a majority of respondents mentioned monitoring accounts in the free-form response questions.

The intention to implement physical security was also driven largely by general identity theft beliefs but was also influenced by the belief that personal documents would be secure.

Practicing password security seems to be driven by opposing beliefs. The belief that proper password practices are required to minimize identity theft was offset by the belief that doing so will impede access to online resources.

The three risky behaviours were all driven by convenience offset by the belief that these behaviours expose one to added identity theft susceptibility. Clicking on a link in an e-mail was driven by the belief that the information will be tailored to the individual, opposed by the belief that the behaviour exposes one to malware and other identity theft outcomes. Giving information over the phone was motivated by the belief that a 'good deal' will be offered, offset by the added risks of identity theft. The belief that using 'remember my password' makes websites easier to use was opposed by the belief that doing so exposes one to added consequences of identity theft.

All behaviour groups were subject to behaviour-specific beliefs to varying degrees.

2) What are the consumer beliefs about factors that help or hinder performance of identity theft prevention and identity fraud detection behaviours that influence perceptions of the ability to perform the behaviours and, in turn, intentions to perform the behaviours?

This research question embodied Hypothesis HT7 (behaviour-specific control beliefs affect PBC), which was supported in two of the analysis groups and marginally supported in a further three (see Table 41 for details). In the 'orthodox' models, PBC was not always successful in explaining a significant portion of intention. The improved models generally dropped or altered the PBC construct and/or directed control beliefs to either intention or behaviour. Control beliefs specific to the studied behaviours had the most significant impacts in the models and each behavioural analysis group had its own set of significant beliefs.

In addition to the general control beliefs of cost and required knowledge, the belief that one can easily find out how to get a credit report had a significant influence on the PBC for getting a credit report.

PBC had a minimal effect on intention to check the land registry office but the belief that knowledge is required directly affected intention.

The belief that an uncomplicated process aids monitoring accounts influenced PBC for monitoring credit cards and bank accounts.

The requirements of a shredder and a secure location to store sensitive documents were significant factors influencing the PBC for physical security.

No behaviour-specific control beliefs affect the PBC for practicing password security, but the beliefs that secure passwords and multiple passwords are hard to remember did moderate actual behaviour.

The control beliefs for risky behaviours do not have a large influence on intention. The belief that just opening and then closing a link poses no danger moderated the behaviour of clicking on a link in an e-mail. Who makes the phone call had a direct influence on the intent to give personal information over the phone. Whether other people use the computer and the belief that 'remember my password' does not always work both influenced the intention to use 'remember my password'.

Behaviour-specific control beliefs had a widely varying impact on intention and ultimately behaviour.

3) What are the consumer beliefs about the influence of significant others toward performance of identity theft prevention and identity fraud detection behaviours that affect inclination to perform behaviours and in turn intentions to perform the behaviours?

This research question aligns precisely with Hypothesis HT5. Subjective norm had a statistically significant influence on the intention to perform the behaviours in the analysis group at the 0.05 level for only two of the groups examined in this study (see section 6.2). In these two cases, the path coefficient was negative, implying that consumers do the opposite to the wishes of significant others although the effect sizes where very small (0.006 and 0.032). The hypotheses was not supported for any analysis groups. The subjective norm construct is generally found to be a weak predictor of intention (Armitage and Conner, 2001). It is possible that, since identity theft prevention and identity fraud detection behaviours can be said to be performed in private, the influence of others is minimal (Boss et al., 2009).

4) Do attitudes and beliefs toward some identity theft prevention and identity fraud detection behaviours affect the intention to perform other identity theft prevention and identity fraud detection behaviours?

As noted in Section 6.2, the attitudes and PBC for one behaviour group had almost no statistically significant effect on the intentions to perform the behaviours in other groups. The low correlations between behaviour components that Gilbert and Archer (2012) observed appear to extend backwards into the attitudes and PBCs that precede them. Attitudes and beliefs toward one behaviour analysis group had virtually no influence on the intention to perform other behaviours.

5) Do consumer beliefs about the consequences and outcomes of identity fraud in general influence attitudes toward specific behaviours and, in turn, intentions to perform the behaviours?

This research question encompassed Hypotheses HT2 (general behavioural beliefs affect attitudes) and HT7 (general control beliefs affect PBC).

HT2 was supported for at least one general belief in three of the analysis groups and marginally supported in a further four. Behavioural beliefs about identity theft in general do not appear, however, to have an overwhelming influence on the attitude toward and subsequently intention to perform behaviours to prevent and detect identity theft and fraud. The belief that behaviours will prevent financial loss, stop criminal activity, or give peace of mind, for example, seemed to have almost no influence at the 0.01 confidence level in the full sample. The general beliefs that behaviours will protect privacy, complicate transactions, avoid the hassle of dealing with fraud, secure personal information, and prevent the loss of reputation all had some statistical impact on the intention to perform at least some of the studied behaviours.

HT7 was supported for at least one behavioural belief in two of the analysis groups and marginally supported in a further three groups. For the purposes of looking at control beliefs, the behaviours studied can be classified into two groups: the three risky behaviours and the other (proactive) behaviours. Control beliefs about identity theft in general had almost no influence on the perceived behavioural control of risky behaviours. The general beliefs that identity theft prevention and identity fraud detection require a lot of knowledge and cost a lot were significant control beliefs in all the proactive behaviours. The belief that diligence is required was a significant control belief for physical security and password behaviours.

6) Which of two theories, TPB or PMT, better models consumer identity theft prevention and identity fraud detection behaviours?

The Theory of Planned Behaviour (TPB) provided some explanations of consumer behaviour. Table 57 provides the R squared values for the major constructs. For attitude, there was an apparent divide between 'risky' behaviours and 'positive' behaviours. For the positive attitudes, R squared values ranged from 0.408 to 0.531, indicating that a substantial portion of the variance in attitude is explained. For the 'risky' behaviours, values ranged from 0.142 to 0.218, suggesting that most of the variance was unexplained. At best, less than one-third of the variation in PBC was explained by the control beliefs for any of the behavioural groups studied. On the other hand, at least half and as much as 0.785 of the variation in intention was explained. Unfortunately, most of the variation in self-reported behaviour remains unexplained.

Table 57 - R Squared Values for TPB Models

Analysis Group	Attitude	PBC	Intention	Behaviour
Credit Report	0.408	0.200	0.698	0.372
Land Registry	0.456	0.215	0.613	0.118
Monitor Accounts	0.477	0.186	0.760	0.233
Physical Security	0.531	0.304	0.629	0.179
Password Security	0.465	0.155	0.785	0.139
Click on Link in E-mail	0.167	0.085	0.541	0.098
Give Personal Information Over the Phone	0.142	0.114	0.567	0.115
Use 'Remember My Password'	0.218	0.159	0.667	0.352

Attitudes toward a behaviour were always influential on the intention to perform that behaviour. The influence of Perceived Behavioural Control (PBC) on intention was less successful. In most cases, it was not a statistically significant predictor of intention. Although intentions were always statistically significant predictors of performance, much of the variation in performance was unexplained.

Table 58 shows the R squared values for intention and behaviour for PMT. As in TPB, intentions were always statistically significant predictors of behaviour. Also as in TPB, much of the variation in behaviour was unexplained with R squared values ranging from 0.088 to 0.362.

Table 58 - R Squared Values for PMT Models

Analysis Group	Intention	Behaviour
Credit Report	0.370	0.362
Land Registry	0.533	0.088
Monitor Accounts	0.678	0.244
Physical Security	0.559	0.234
Password Security	0.744	0.129
Click on Link in E-mail	0.306	0.116
Give Personal Information Over the Phone	0.341	0.173
Use 'Remember My Password'	0.355	0.352

As shown in the R squared values, the PMT models always explained less of the variation in intention than TPB. The addition of the attitude construct in TPB between the behavioural beliefs and the intention construct provided higher explanatory power for intention than the direct connection between beliefs and intention in PMT. The TPB requirement that behaviours should be narrowly specified, however, limited its general applicability. Neither theory explained the disconnect between intention and actual behaviour. For the most part, consumers were well intentioned, so understanding the gap between intention and behaviour is key to understanding behaviour. While TPB seems to be a slightly better model in that it surfaced more of the salient beliefs and explained more of the intention, neither TPB nor PMT explains as much of the behaviours as might be desired.

7) Do consumers consider credit card fraud less threatening than other identity fraud?

As observed in Chapter 2, there is some discussion as to whether credit card fraud should be considered an identity crime due to the limited amount of personal information stolen and the usually minimal consequences. As noted in Chapter 9, a substantial majority of consumers believed that credit card fraud is just as serious and causes as much worry as other identity fraud. It would seem that, in the minds of consumers, credit card fraud is an identity crime.

10.2 Limitations

There are several potential limitations to the study pertaining to the sample, the length of the Phase 2 survey and the methods used.

The Phase 2 (primarily quantitative) survey was conducted online using a standing panel maintained for commercial purposes. That circumstance may have biased the sample. It certainly excluded people without Internet connections. This is not as large a limitation as it once was. According to Statistics Canada, 80.3% of individual Canadians used the Internet for personal reasons during 2009, up from 67.9% during 2005 (Statscan, 2013). The kind of people retained by the survey company may be biased in some way, although the company attempts to maintain a representative population. While attempts were made to generate a representative sample, there was a bias toward younger females. The age bias was possibly due to the use of the Internet survey and the bias toward females was the result of their greater perseverance. The demographics of the sample were nonetheless reasonably close to that of the Canadian population (see Appendix F). The survey was conducted in Canada, which may limit its generality in other locations.

The length of the survey may have been a biasing factor: 176 respondents abandoned the survey without completing it. (These observations were not included in any of the analysis, with the exception of the qualitative analysis.) The sort of person that persevered to the end may be unrepresentative. The average time for completion, however, was only slightly over the maximum of 30 minutes recommended by Fowler (2001, p103). To reduce the length, many of the reflective latent variables started out with only three items. When one of these was non-convergent and dropped, the latent variable was left with only two indicators, potentially compromising validity.

The use of self-reported behaviour necessitated by the survey vehicle may not reflect actual behaviour. Ideally, actual behaviour would be measured immediately after the survey but given the anonymous Internet administration, this was not possible. There are indications that self-reported behaviour is a reasonable proxy for actual behaviour. In an experimental TPB study employing both observed and self-reported behaviours, Elliot et al. (2007) found strong correlations between self-reported and observed behaviour. Armitage and Conner (2001), in a meta-analysis of 63 TPB studies that considered the difference between studies that used self-reported behaviour and those that used observed behaviour, noted that

> "The TPB accounts for large, highly significant proportions of the variance in prospective measures of both observed ($R^2 = .20$) and self-reported ($R^2 = .31$) behaviour. Although this difference is significant (qs = .14, p<.01), it is encouraging that the TPB can account for considerable proportions of the variance in actual behaviour (i.e. a medium-large effect size)"

As noted in the qualitative analysis in Chapter 8, the 'observer effect' changed the participants' perceptions during the survey because the questions presented new information. The extent of this effect is not known and difficult to quantify.

10.3 Further Research

The hypotheses on which this research is based assumed that the belief system around identity theft and fraud in general would have a significant influence on the intention to perform prevention and detection behaviours. Much of the survey instrument was devoted to identity theft in general rather than to specific behaviours. This research shows, however, that beliefs about identity theft in general do not have overwhelming influence on the intention to perform specific behaviours or behavioural components. Furthermore, the beliefs about one behaviour or behavioural component have minimal influence on the intent to perform another behaviour or behavioural component. Given that the majority of the variation in behaviour in all of the models is unexplained, more detailed research on individual behavioural components is in order. Since these components are largely orthogonal, each can be considered without respect to other behavioural components.

If identity theft prevention and identity fraud detection behaviours are to be better understood, more research is needed into the connection between intention and behaviour. Most respondents were aware of the possibility and the bad consequences of identity theft and they had intentions to perform appropriate behaviours to avoid and detect identity theft, but these intentions did not strongly correlate with behaviours. Self-control literature fits with the identity theft behaviour context. Originally defined as 'effortful impulse inhibition', self-control has been studied in such contexts as dieting (avoiding chocolate cake or other inappropriate foods) and smoking (Fujita, 2011). More recently, self-control has been defined as situations where 'short-term outcomes are in opposition to long-term outcomes' (Trope and Fishbach, 2000). The essence of identity theft protection is balancing short-term behaviours (monitoring accounts and avoiding risky behaviours, for example) against obtaining long-term benefits (avoiding identity theft). There are some interesting findings in self-control research that may illuminate the connection between identity theft intentions and behaviours. Iso-Ahola (2012), for example, states that "If the enduring goal ... is based on extrinsic factors or internal pressures ('I should'), then it is more easily interrupted by perceived constraints than if it reflects true choice and desire." Practicing secure password behaviour, for example, is unlikely to be based on intrinsic rewards, which suggests that behaviours are susceptible to interruption, thus weakening the link between intention and behaviour. A further insight from the self-control research is that the relationship between intention and behaviour is weak for those who perform the behaviour habitually (Chatzisarantis and Hagger, 2007), suggesting that, for example, assuming that monitoring accounts is habitual, the connection between the intention and behaviour will be weak, as was observed in this study. (The R squared for the monitoring credit cards behaviour was only 0.16). The most prominent theory in the self-control literature appears to be that of the Transtheoretical Model (TTM) proposed originally by Prochaska and DiClemente (1983, 1984) and reviewed by Armitage (2009). It is a popular theory in health behavioural change (a search on 'Web of Science' found 1,470 articles with Transtheoretical Model in either the title or topic and all but 63 were in the health field). TTM defines one dependent and 14 independent variables and proposes that behavioural change is a process of five stages: precontemplation, contemplation, preparation, action, and maintenance. The application of TTM or other self-control theories to identity theft prevention and identity fraud detection behaviours could provide a better understanding of the gap between intentions and behaviours.

Although Milne et al. (2004) noted demographic aspects to online privacy, the cultural and demographic differences that came to light in the analysis of identity crime qualitative belief data were unexpected and could be the basis of further research.

In summary, each identity theft prevention and detection behaviour group could and should be studied in isolation from other behaviour groups, since beliefs and attitudes toward one group have little influence on the intention to perform other groups and since many of the significant beliefs are specific to the behaviour group. In general, consumers are well intentioned but fail to perform. The application of self-control theories such as TTM may provide better insight into the gap between intention and behaviour that is key to creating interventions to improve performance. Demographic and cultural dimensions should be included in any future research.

10.4. Conclusion

Identity theft and identity fraud are considerable problems in Western societies and can be particularly devastating for individual victims. While governments can legislate against identity crimes and organizations can safeguard the information they hold, individuals continue to play a critical role in preventing identity theft and detecting identity fraud. On the whole, consumers are concerned about identity theft and fraud but do not always behave in their best interests. This research helped to understand the behaviours of consumers in the context of identity theft and identity fraud.

Identity theft prevention is analogous to disease prevention. To prevent disease, an individual must have a proper diet, get exercise, get enough rest, and get appropriate immunization. Each of these areas has its own set of behaviours. To minimize the chances of disease, individuals must use all of the disease prevention behaviours but even then a disease-free life is not guaranteed. So it is with identity theft behaviours. Practicing password security alone will not prevent identity theft nor will using physical security or avoiding risky behaviours. Consumers need to exercise all positive behaviours and avoid all risky behaviours if they are to minimize their exposure to identity theft and fraud.

Individuals are well aware of their vulnerability to identity theft if they take no precautions to prevent it. Furthermore, they believe the consequences of identity fraud to be severe. These convictions appear to have some influence on the intention to perform specific behaviours, but behaviour-specific beliefs appear to be, in general, just as influential. For example, the two behaviours in the 'monitoring agencies' component ('checking the land registry' and 'getting a credit report annually') seem to not be as associated with identity theft detection as other behaviours, since in both cases the belief that the behaviour had no benefit was significant. The three risky behaviours also stood out in that control beliefs were not generally significant. It appears as if control as defined in TPB (i.e., the ability to perform the behaviours) is not particularly applicable, since the risky behaviours are designed to be easy to use. The circumstances in which the behaviour may be performed seem to be more pertinent. Identity theft prevention and identity fraud detection behaviours cannot be understood without taking into account the beliefs that are specific to each group of behaviours.

Attitudes toward behaviours to prevent identity theft and identity fraud appear to be isolated; i.e., the positive attitudes toward one type of behaviour affect the intention to perform that behaviour but have virtually no effect on the intention to perform other types of behaviours. The orthogonality in behaviours documented by Gilbert and Archer (2012) appears to extend 'upstream' into the belief systems of consumers. These findings suggest that efforts directed at influencing consumer behaviour to prevent identity theft should be directed at all the specific behaviours or behavioural components rather than at identity theft in general.

The consistency tenets of TPB hold that the behaviour under study should be strictly defined in action, target, context, and time. By leaving the context out of the model, TPB generates limited models that can be applied only in very narrow circumstances. The alteration of the 'orthodox' TPB models to include context as an influence on intention, behaviour or as moderators to the path between intention and behaviour made marked improvements to the models.

Protection Motivation Theory (PMT) was similar in effect to TPB in that intention to perform the behaviour was a significant influence of the actual performance of the behaviour. It too failed to explain most of the variation in behaviour. Of particular note is the finding that the perception of vulnerability and severity of identity theft and fraud in general had little effect on the intention to perform the behaviour. Almost all of the effective elements were specific to the behaviour.

Neither TPB nor PMT provides a complete model of identity theft prevention and identity fraud detection behaviours. The moderate connection between the intention and self-reported behaviour in all of the behavioural groupings suggests that there are factors (other than intention, and in the case of TPB, perceived behavioural control) that have significant influence on behaviour. Finding these factors is key to understanding identity theft prevention and identity fraud detection behaviours.

Gilbert and Archer (2012) demonstrated that identity theft prevention and detection behaviours when reduced to principal components are almost orthogonal; that is, performing the behaviours in one component has little correlation with the performance of other behavioural components. This study extends that isolation back into the predecessor attitude and control beliefs. The finding that positive attitudes and positive control beliefs toward one behaviour component have almost no influence on the intention to perform other behavioural components is a new understanding in the identity theft prevention and detection behavioural field.

Taken together, these findings have significant implications for those practitioners seeking to enhance identity theft prevention and detection behaviours. They suggest that stressing the impact of identity theft in general will have little effect. First of all, consumers already seem well aware of the severity of and vulnerability to identity theft and fraud (see the PMT general vulnerability and severity statistics and associated graphs in Appendix J and Appendix K, respectively). Furthermore, these general perceptions have a moderate effect on the intention to perform specific behaviours. Practitioners should concentrate on the beliefs that underlie the attitudes toward specific behaviours. For example, two of the beliefs that had a significant influence on attitudes toward checking the land registry were the belief that it is required only when buying or selling a house and the belief that it has no benefit. These findings suggest that communications with consumers should aim to correct these behaviour-specific perceptions. Practitioners also need to stress with consumers that they should undertake *all* the appropriate behaviours. Using the physical measures of shredding confidential waste, using a locked mailbox and keeping confidential documents in a safety deposit box will not prevent identity thieves from obtaining your password, taking out a mortgage on your home, opening a line of credit with your ID, or putting purchases through on your credit card number.

Given that there were only three items, the qualitative data proved to be an unexpectedly rich source of new information. The discovery of the issues of most concern to consumers and their views on the best measures to prevent identity theft and detect identity fraud were illuminating and tended to corroborate the findings in the quantitative portion of the survey. The discovery of the significant demographic factors that impacted on these issues was unexpected. French speakers are less likely to be concerned about online transactions, less likely to consider monitoring their credit cards and banks accounts and checking their credit reports as key to detecting identity fraud, and more likely to profess to not knowing how to detect identity fraud than English speakers. Men are less likely to be concerned about online transactions and less likely to consider monitoring their bank accounts and credit cards as crucial than women. Older consumers are less likely to be concerned about online transactions, more likely to be concerned about how institutions handle their information, and more likely to be concerned about 'phishing' than younger consumers.

As the first attempt at a comprehensive model of the behaviours of consumers as they try to prevent identity theft and detect identity fraud, this research has brought new insights and practical implications:

1) Beliefs about one type of behaviour have little impact on the intent to perform other types of behaviour. Individual behaviour components can be studied independently. Practitioners should emphasize that consumers need to perform all prevention and detection behaviours.

2) The intent to perform one type of behaviour is motivated at least as much by beliefs about that type of behaviour as by beliefs about identity theft in general. In addition to emphasizing the potential for identity theft and the consequences of identity fraud, practitioners should concentrate on encouraging individual behaviours.

3) There are cultural and demographic differences in beliefs about identity theft prevention and identity fraud detection behaviours. Practitioners need to tailor their interventions based on the beliefs specific to the targeted demographic segment.

4) Much of the variation in reported behaviour is unexplained by the intent to perform the behaviour. Future work is needed to define the factors that affect behaviours.

References

Abraham, C.S., Sheeran, P., Abrams, D. and Spears, R. (1994) Exploring teenagers' adaptive and maladaptive thinking in relation to the threat of HIV infection, *Psychology and Health*, 9, 253-272.

Acquisti, A. Friedman, A. and Telang, R. (2006). Is there a cost to privacy breaches? An event study, Fifth Workshop on the Economics of Information Security, University of Cambridge, England, June.

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

Ajzen, I. and Madden, T. J. (1986). Prediction of goal-directed behavior: Attitudes, intentions, and perceived behavioral control, *Journal of Experimental Social Psychology*, 22, 453-74.

Ajzen, I., Brown, T. C. and Carvajal, F. (2004). Explaining the discrepancy between intentions and actions: The case of hypothetical bias in contingent valuation, *Personality and Social Psychology Bulletin*, 30, 1108-21.

Ajzen, Icek (2005). *Attitudes, Personality and Behavior*, 2nd ed., McGraw-Hill International (UK) Ltd, Maidenhead.

Ajzen (2009a) TPB Questionnaire Construction http://people.umass.edu/aizen/pdf/tpb.measurement.pdf accessed June 20, 2011.

Ajzen (2009b) TPB Diagram http://people.umass.edu/aizen/tpb.diag.html accessed December 19, 2011.

Anderson, Janna Quitney and Rainie, Lee (2010) Millenials will make online sharing in networks a lifelong habit, *Pew Research Center's Internet & American Life Project*, http://www.pewinternet.org/~/media//Files/Reports/2010/PIP_Future_Of_Millennials.pdf accessed June 15, 2011.

Anderson, J. C., and Gerbing, D.W., (1988). Structural Equation Modeling in Practice - a Review and Recommended 2-Step Approach, *Psychological Bulletin*, Volume 103, Issue 3, pp411-423.

Anderson, Keith B., Durbin, Erik and Salinger, Michael (2008). Identity theft, *Journal of Economic Perspectives*, Vol. 22, No. 2, pp171-192.

Anderson, C. L., & Agarwal, R. (2010). Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions, *MIS Quarterly*, 34(3), 613-A15.

Allen, B. (1993). Frightening information and extraneous arousal: Changing cognitions and behavior regarding nuclear war, *Journal of Social Psychology*, 133, 459-467.

Arachchilage, Nalin Asanka Gamagedara and Love, Steve (2013). A game design framework for avoiding phishing attacks, *Computers in Human Behavior,* Volume 29, Issue 3, May , pp706-714.

Armitage, C.J. and Conner, M. (2001) Efficacy of the theory of planned behaviour: A meta-analytic review, *British Journal of Social Psychology*, Vol. 40, Dec, 471-499.

Armitage, C. J. (2009), Is there utility in the transtheoretical model?. *British Journal of Health Psychology*, 14: 195–210.

Australian Payments Clearing Association (2012) Fraud Statistics 2012 Financial Year http://apca.com.au/docs/fraud-statistics/payment-fraud-statistics-financial-year-2012.pdf accessed February 21, 2013.

Bamberg, Sebastian and Möser, Guido (2007). Twenty years after Hines, Hungerford, and Tomera: A new meta-analysis of psycho-social determinants of pro-environmental behaviour, *Journal of Environmental Psychology*, Volume 27, Issue 1, March, Pages 14-25.

Barclay, D., Thompson, R. and Higgins, C. (1996) The Partial Least Squares (PLS) Approach to Causal Modeling: Personal Computer Adoption and Use an Illustration, Technology Studies 2, 20, pp. 285-309.

Ben-Ahron, V, White , D. and Phillips, K. (1995). Encouraging drinking at safe limits on single occasions: The potential contribution of protection motivation theory, *Alcohol and Alcoholism*, 30(5), 633-639.

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

Boss, Scott R, Kirsch, Laurie J, Angermeier, Ingo, Shingler, Raymond A and Boss, R Wayne (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security, *European Journal of Information Systems*, Vol. 18, Issue 2, pp 151-164.

Bowie, N. E., and Jamal, K. (2006). Privacy Rights on the Internet: Self-Regulation or Government Regulation?. *Business Ethics Quarterly*, 16(3), 323-342.

Box, G. E. P. (1949). A General Distribution Theory for a Class of Likelihood Criteria, *Biometrika*, Vol. 36, No. 3/4 (Dec), pp. 317-346

Brennan, R. L. and Predinger, D. J. (1981). Coefficient Kappa: some uses, misuses, and alternatives, *Educational and Psychological Measurement*, 41, 687-699.

Brodkin, J. (2007). Victims of ChoicePoint data breach didn't take advantage of free offers. Network World, April 10. http://www.networkworld.com/news/2007/041007-choicepoint-victim-offers.html accessed June 15, 2011.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness. *MIS Quarterly*, 34(3), 523-A7.

Canada Post (2013). Canada Post Annual Report 2012, http://www.canadapost.ca/cpo/mc/assets/pdf/aboutus/annualreport/2012_AR_complete_en.pdf, accessed December 11, 2013.

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

Chatzisarantis, N. L. and Hagger, M. (2007). Mindfulness and the intention - behavior relationship within the theory of planned behavior, *Personality and Social Psychology Bulletin*, 33, 663-676.

Chin, W. W., and Newsted, P. (1999). Structural equation modeling analysis with small samples using partial least squares, *Statistical strategies for small sample research*, 307-341.

Chin, W. W. (1998). The Partial Least Squares Approach to Structural Equation Modeling, in G. A. Marcoulides (Ed.) *Modern Methods for Business Research*, London, pp. 295-236.

Chiquoine, B., and Hjalmarsson, E. (2009). Jackknifing stock return predictions. *Journal of Empirical Finance*, 16(5), 793-803.

CIRA (2013). CIRA Fact Book 2013, Canadian Internet Registration Authority, http://www.cira.ca/factbook/2013/canada-online.html accessed Feb 15, 2014.

Coggeshall, Stephen (2007), ID Theft Knows No Boundaries, eCommerce Times, April 13, 2007, http://www.ecommercetimes.com/story/56864.html accessed Sept 14, 2011.

Cohen, J. (1960). A coefficient of agreement for nominal scales, *Educational and psychological measurement*, 20, 37-46.

Cohen, J. (1988). Statistical power analysis for the behavioral sciences (2nd ed.). Hillsdale, N.J.: Lawrence Erlbaum Associates.

Cohen, Lawrence E. and Felson, Marcus (1979). Social Change and Crime Rate Trends: A Routine Activity Approach, *American Sociological Review*, Vol. 44, No. 4, pp. 588-608.

Conner, M. and Norman, P. (2005) Predicting Health Behaviour: A Socil Cognition Approach, in: Conner, M. and Norman, P., editors *Predicting Health Behaviour*, 2nd ed. London: Open University Press, pp1-27.

Chollet, G., Perrot, P., Karam, W., Mokbel, C., Kanade, S., and Petrovska-Delacret, D. (2012). Identities, forgeries and disguises. *International Journal of Information Technology & Management*, 11(1), 138-152.

Conner, M. and McMillan, B. (1999). Interaction effects in the theory of planned behaviour: Studying cannabis use, *British Journal of Social Psychology*, 38, 195-222.

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 July 14, 2010.

Consumers Union (2008) Consumers' Union Guide to Security Freeze Protection, http://www.consumersunion.org/campaigns/learn_more/003484indiv.html Accessed Sept 19, 2011.

Cooke, Richard and French, David P.(2008). How well do the theory of reasoned action and theory of planned behaviour predict intentions and attendance at screening programmes? A meta-analysis, *Psychology & Health*, Vol. 23, Iss. 7.

Council of Europe. (2001). Convention on Cybercrime http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm (accessed March 13, 2011). Budapest, Hungary: Council of Europe.

Courneya, K. S. (1995). Understanding readiness for regular physical activity in older individuals: An application of the theory of planned behavior, *Health Psychology*, 14, 80-87.

Cronbach, L. J. (1951). Coefficient alpha and the internal structure of tests. *Psychometrika*, 16, 297-334.

Davis, Fred D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology, *MIS Quarterly* 13, no. 3: 319-340.

Davis, L. E., Ajzen, I., Saunders, J. and Williams, T. (2002) The decision of African American students to complete high school: An application of the theory of planned behavior, *Journal of Educational Psychology*, 94, 810-19.

Department of Justice (2010). Tougher Laws Targeting Identity Theft Come Into Force, http://www.justice.gc.ca/eng/news-nouv/nr-cp/2010/doc_32470.html accessed January 8, 2014.

Dinev, T., Goo, J., Hu, Q., and Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal*, 19(4), 391-412.

National Cyber Security Alliance (2009), Home User Study October 2009, http://www.staysafeonline.org/sites/default/files/resource_documents/Home%20User%20Study%20FINAL.pdf accessed Sept 14, 2011.

East, R. (1993). Investment decisions and the theory of planned behavior, *Journal of Economic Psychology*, 337-75.

Efron, B., Rogosa, D., and Tibshirani, R. (2004). Resampling methods of estimation. In N.J. Smelser, and P.B. Baltes (Eds.). *International Encyclopedia of the Social & Behavioral Sciences* (pp. 13216-13220). New York, NY: Elsevier.

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

Elliott, Mark A., Armitage, Christopher J. and Baughan, Christopher J. (2007). Using the theory of planned behaviour to predict observed driving behaviour, *British Journal of Social Psychology*, Vol. 46, Iss. 1, p69-90.

Featherman, Maurice S. and Pavlou, Paul A. (2003). Predicting e-services adoption: a perceived risk facets perspective, *International Journal of Human-Computer Studies,* 59 451-474.

Federal Trade Commission (2006) Take Charge: Fighting Back Against Identity Theft, http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.pdf, accessed August 14, 2010

Federal Trade Commission (2011) FTC Releases List of Top Consumer Complaints in 2010; Identity Theft Tops the List Again http://www.ftc.gov/opa/2011/03/topcomplaints.shtm accessed January 10, 2012

Federal Trade Commission (2013) Consumer Sentinal Network Databook for January - December 2012, http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2012.pdf accessed July 3, 2013

Fisk, S. M., and Stigile, C. (2012). Will the Real John Doe Please Stand Up?: Tax Identity Theft Developments. *Journal Of Tax Practice & Procedure*, 14(1), 21-71.

Fishbein, M. (1963). An investigation of the relationships between beliefs about an object and the attitude toward that object. *Human Relations*, 16, 233-239.

Fleiss, J. L. (1981). *Statistical Methods for Rates and Proportions*. John Wiley & Sons.

Floyd, Donna L., Prentice-Dunn, Steven and Rogers, Ronald W. (2000), A Meta-Analysis of Research on Protection Motivation Theory, Journal of Applied Social Psychology, 30(2).

Fornell, C. and Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error, *Journal of marketing research*, 18(1), 39-50.

Fowler, Jr., F. J. (2001). Survey Research Methods (3rd. Ed). *Applied Social Research Methods Series*, Vol. 1. Newbury Park, CA: Sage.

Fujita, Kentaro (2011). On Conceptualizing Self-Control as More Than the Effortful Inhibition of Impulses, *Personality And Social Psychology Review*, Nov, Vl 15, Is 4, 352-366.

Furletti, Mark and Smith, Stephen (2005) The Laws, Regulations, and Industry Practices That Protect Consumers Who Use Electronic Payment Systems: Credit and Debit Cards, Federal Reserve Bank of Philadelphia Payment Cards Center Discussion Paper 50-01.

Funk, Josh (2007) Contact Data for millions of AMeritrade Customers Stolen, *Kansas City Star*, September 14,2007, http://kansascity.com/business/vprint/story/276100.html.

Gefen David, Straub, Detmar W. and Boudreau, Marie-Claude (2000) - Structural Equation Modeling and Regression: Guidelines for Research Practice, *Communications of the Association for Information Systems*, Vol. 4, No. 7, October.

Gilbert, John and Archer, Norm (2012) Consumer identity theft prevention and identity fraud detection behaviours, *Journal of Financial Crime*, Vol. 19 Iss: 1, pp.20 - 36.

Giles, M. and Cairns, E. (1995). Blood donation and Ajzen's theory of planned behaviour: An examination of perceived behavioural control, *British Journal of Social Psychology*, 34, 173-88.

Goodhue, D. L., Lewis, W., and Thompson, R. (2012). Does PLS Have Advantages For Small Sample Size or Non-Normal Data?. *MIS Quarterly*, 36(3), 981-A16.

Griffeth, R. W. and Rogers, R. W. (1976). Effects of fear-arousing components of driver education on students' safety attitudes and simulator performance, *Journal of Educational Psychology*, 68. 501-506.

Gwet, K. L. (2008). Computing inter-rater reliability and its variance in the presence of high agreement, *British Journal of Mathematical and Statistical Psychology*, 61, 29-48.

Hagger, M. S. and Chatzisarantis, N. L. D. (2009), Integrating the theory of planned behaviour and self-determination theory in health behaviour: A meta-analysis. *British Journal of Health Psychology*, 14: 275–302.

Hair, J.F., Anderson, R.E., and Tatham, R.L. (1987). *Multivariate data analysis*. New York, NY: Macmillan.

Hair, J. F. Jr., Andersen, R. E., Tatham, R. L. and Black, W. C. (1998) *Multivariate Data Analysis with Readings*, 5th Edition. Englewood Cliffs, NJ, Prentice Hall.

Hair, J. F., Black, W.C., Babin, B.J., and Anderson, R.E. (2009). *Multivariate data analysis*. Upper Saddle River, NJ: Prentice Hall.

Hair, J. F., Black, W. C., Babin, B. J., and Anderson, R. E. (2010). *Multivariate Data Analysis: A Global Perspective (7th ed.)*. Upper Saddle River: Pearson Prentice Hall.

Hass, J. W., Bagley, G. S. and Rogers, R. W. (1975). Coping with the energy crisis: effects of fear appeals upon attitudes toward energy consumption, *Journal of Applied Psychology*, 60, 754-756.

Hausenblas, H.A., Carron, A.V. and Mack, D.E. (1997). Application of the theories of reasoned action and planned behavior to exercise behavior: A meta-analysis, *Journal of Sport & Exercise Psychology*, March, VL 19,IS 1, pp36-51.

Henseler, J., and Chin, W. W. (2010). A comparison of approaches for the analysis of interaction effects between latent variables using partial least squares path modeling. *Structural Equation Modeling*, 17(1), 82-109.

Herath, T., and Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106-125.

Hrubes, D., Ajzen, I. and Daigle, J (2001). Predicting hunting intentions and behavior: An application of the theory of planned behavior, *Leisure Sciences*, 23, 165-78.

Identity Theft Resource Center (2012). 2011 Data Breadth Stats, http://www.idtheftcenter.org/artman2/uploads/1/ITRC_Breach_Stats_Report_2011_20120207.pdf accessed June 19, 2012

Information Management (2010), TJX Hacker Gets 20 Years, *Information Management Journal*; Vol. 44 Issue 5 Sep/Oct, pp15-15.

Institute for Prospective Technological Studies (2005) Biometrics at the Frontiers: Assessing the impact on Society, *European Commission Joint Research Centre*, February.

Interpol. (2010). Payment cards. Lyon, France. The International Criminal Police Organization.

Isikoff, Michael (2009). Bernanke Victimized by Identity Fraud Ring, *Newsweek*, Aug 24, 2009 http://www.thedailybeast.com/newsweek/2009/08/24/bernanke-victimized-by-identity-fraud-ring.html accessed June 18, 2012

Iso-Ahola, S. (2013). Exercise: Why it is a challenge for both the nonconscious and conscious mind, *Review of General Psychology*, 17(1), 93-110.

Jackson, M. and Ligertwood, J. (2006). Identity management: is an identity card the solution for Australia?, *Prometheus*, 4, 379-387.

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

Jamieson, Rodger, Pek Wee Land, Lesley, Winchester, Donald, Stephens, Greg, Steel, Alex, Maurushat, Alana and Sarre, Rick (2012). Addressing identity crime in crime management information systems: Definitions, classification, and empirics, *Computer Law & Security Review*, Volume 28, Issue 4, August, Pages 381-395.

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

Kepner, T. (2012) "Identity Fraud Problem Could Be More Widespread." *New York Times*, Janurary 9, page: SP11.

Klein, Allison (2010), 18- to 24-year-olds most at risk for ID theft, survey finds, *Washington Post*, March 17, http://www.washingtonpost.com/wp-dyn/content/article/2010/03/16/AR2010031604209.html accessed June 15, 2011.

Koops, Bert-Jaap, Leenes, Ronald Meints, Martin ,van der Meulen, Nicole and Jaquet-Chiffelle, David-Olivier, (2009) A Typology Of Identity-Related Crime, *Information, Communication & Society*; Vol. 12, Issue 1, pp1-24.

Kreuter, Eric A. (2003). The impact of identity theft through cyberspace. *The Forensic Examiner*, 5-6, pp30-35.

Kreuter, Eric A. (2004). Psychopathic Criminal's Behavior as the Wheels of Justice Slowly Turn. *The Forensic Examiner*, 4, pp28-35.

Kunick, J. M. and Posner, N. B. (2011) Following the red flag rules to detect and prevent identity theft. *Information Management Journal*, (Vol. 45). (3), 25.

Lai, Fujun, Li, Dahui and Hsieh, Chang-Tseh, (2012). Fighting identity theft: The coping perspective, *Decision Support Systems*, Volume 52, Issue 2, January, Pages 353-363.

Landis, J. R. and Koch, G. (1977). "The measurement of observer agreement for categorical data", *Biometrics*, 33, 159-174.

Langton, Lynn and Baum, Katrina (2010) "Identity Theft Reported by Households, 2007 - Statistical Tables", Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice, http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh07st.pdf , accessed June 28, 2011.

Langton, Lynn (2011) Identity Theft Reported by Households, 2005-2010, Bureau of Justice Statistics, Office of Justice Programs, U.S. Department of Justice http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh0510.pdf accessed January 10, 2012.

Lee, D., Larose, R., and Rifon, N. (2008). Keeping our network safe: a model of online protection behaviour. *Behaviour & Information Technology*, 27(5), 445-454.

Lee, M. (2009). Factors influencing the adoption of internet banking: An integration of TAM and TPB with perceived risk and perceived benefit. *Electronic Commerce Research & Applications*, 8(3), 130-141.

Lee, S., Song, X. Y., and Poon, W. (2004). Comparison of approaches in estimating interaction and quadratic effects of latent variables. *Multivariate Behavioral Research*, 39(1), 37-67.

Lee, Y., and Kozar, K. A. (2005). Investigating Factors Affecting the Adoption of Anti-Spyware Systems. Communications Of The ACM, 48(8), 72-77.

Lee, Y. (2011). Understanding anti-plagiarism software adoption: An extended protection motivation theory perspective. *Decision Support Systems*, 50(2), 361-369.

Lersch, K. M., and Hart, T. C. (2011). *Space, time, and crime (3rd ed.)*, Durham, N.C.: Carolina Academic Press.

Lilliefors, Hubert W. (1967). On the Kolmogorov-Smirnov Test for Normality with Mean and Variance Unknown, *Journal of the American Statistical Association*, Vol. 62, No. 318, pp. 399-402.

Lüdemann, C. (1997) Rationalität und Umweltverhalten, Weisbaden: Deutscher Univerisitäts-Verlag.

Micceri, T. (1989). The Unicorn, the Normal Curve, and Other Improbable Creatures. *Psychological Bulletin*, 105(1), 156-166.

Milne, George R., Rohm, Andrew J. and Bahl, Shalini (2004). Consumers' Protection of Online Privacy and Identity. *Journal of Consumer Affairs*, 2, pp217-232.

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

Milne, S., Sheeran, P., and Orbell, S. (2000). Prediction and intervention in health-related behavior: A meta-analytic review of protection motivation theory. *Journal of Applied Social Psychology*, 30(1), 106-143.

Milne, S., Orbell, S., and Sheeran, P. (2002). Combining motivational and volitional interventions to promote exercise participation: Protection motivation theory and implementation intentions. *British Journal of Health Psychology*, 7(2), 163-184.

Munoz, Y., Chebat, J., and Suissa, J. A. (2010). Using fear appeals in warning labels to promote responsible gambling among VLT players: The key role of depth of information processing. *Journal of Gambling Studies*, 26(4), 593-609.

Murphy, Samantha (2008), Online security crackdown: scanning service oversees site security at David's Bridal, *Chain Store Age* July: 46.

National Cyber Security Alliance (2009). 2009 NCSA / Symantec Home User Study, October, http://www.staysafeonline.org/sites/default/files/resource_documents/Home%20User%20Study%20FINAL.pdf accessed Sept 14, 2011.

National Cyber Security Alliance (2011). 2011 NCSA / McAfee Home User Study, October, http://www.staysafeonline.org/download/datasets/2068/#sthash.16a6cgro.dpuf accessed June 7, 2012.

Neumann, Peter G. (2000). Kevin Mitnick testifies before Congress, PoliTech: Politics & Technology, http://www.politechbot.com/p-00969.html accessed July 3, 2012.

Nevitt, J., and Hancock, G.R. (2001). Performance of bootstrapping approaches to model test statistics and parameter standard error estimation in structural equation modeling. *Structural Equation Modeling*, 8(3), 353-377.

Newman, Graeme R. and McNally, Megan M. (2007) Identity Theft - A Research Review, National Institute of Justice, http://www.ncjrs.gov/pdffiles1/nij/218778.pdf, accessed June 28, 2011.

Newman, Graeme R. and McNally, Megan M. (2005) Identity Theft Literature Review, U.S. Department of Justice, http://www.ncjrs.gov/pdffiles1/nij/218778.pdf accessed June 28, 2011.

Ng, Boon-Yuen , Kankanhalli, Atreyi and Xu,Yunjie (Calvin) (2009). Studying users' computer security behavior: A health belief perspective, *Decision Support Systems*, Volume 46, Issue 4, Pages 815-825.

Norberg, Patricia A., Horne, Daniel R. and Horne, David A. (2007). The privacy paradox: Personal information disclosure intentions versus behaviors, *Journal of Consumer Affairs*, 1, pp100-126.

Norman, p., Boer, H. and Seydel, E. (2005) Protection motivation theory, in: Conner, M. and Norman, P., editors *Predicting Health Behaviour*, 2nd ed. London: Open University Press, pp81-126.

Nunnally, J.C., and Bernstein, I.H. (1994). *Psychometric theory*. New York, NY: McGraw-Hill.

Nunnally, J.C. (1978). *Psychometric theory*. New York, NY: McGraw Hill.

OECD (2009), Online Identity Theft, OECD Paris, http://www.oecd-ilibrary.org/science-and-technology/online-identity-theft_9789264056596-en accessed June 30, 2010.

Office of the Privacy Commissioner of Canada (2009) Identity Theft and You, http://www.priv.gc.ca/information/pub/guide_idt_e.pdf accessed June 30, 2010.

Plotnikoff, R. C., and Trinh, L. (2010). Protection motivation theory: Is this a worthwhile theory for physical activity promotion? *Exercise and Sport Sciences Reviews*, 38(2), 91-98.

Prochaska, J. O. and DiClemente, C. C. (1983). Stages and processes of self-change in smoking: Toward an integrative model of change, *Journal of Consulting and Clinical Psychology*, 51, 390-395.

Prochaska, J. O. and DiClemente, C. C. (1984). *The transtheoretical approach: Crossing the traditional boundaries of change*, Homewood IL: J. Irwin.

Punch, Linda (2004), The New Fraudsters, *New York*, 17, 8, 20-28.

Rhodes, R. E., and Dickau, L. (2012). Experimental evidence for the intention–behavior relationship in the physical activity domain: A meta-analysis. *Health Psychology*, 31(6), 724-727.

Rifon, Nora J., LaRose, Robert and 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.

Rippetoe, P. A., and Rogers, R. W. (1987). Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat. *Journal of Personality and Social Psychology*, 52(3), 596-604.

Rodgers, W. M., Conner, M. and Murray, T. C. (2008), Distinguishing among perceived control, perceived difficulty, and self-efficacy as determinants of intentions and behaviours. *British Journal of Social Psychology*, 47: 607–630.

Rogers, Ronald W. (1975) A protection motivation theory of fear appeals and attitude change, *Journal of Psychology* 91:1 (Sept) pp93.

Rogers, R. W. (1983) Cognitive and psychological processes in fear appeals and attitude change: A revised theory of protection motivation in J. T. Cavioppo and R.E. Petty (Eds.), *Social psychophysiology* (pp. 153-176), Guilford Press, New York.

Romanosky, Sasha, Telang, Rahul and Acquisti, Alessandro (2011) Do data breach disclosure laws reduce identity theft?, *Journal of Policy Analysis & Management*; Spring2011, Vol. 30 Issue 2, pp256-286

Rosenthal, R. R. (1984). *Meta-analytic procedures for social research*, Beverly Hills, CA: Sage.

Sasse, M.A., Brostoff, S, and Weirich, D. (2001). Transforming the 'weakest link' - a human/computer interaction approach to usable and effective security, *BT Technology Journal*, Vol 19, Issue 3, pp 122-131

Sawyer, A. G., and Ball, A. (1981). Statistical Power and Effect Size in Marketing Research. *Journal Of Marketing Research (JMR)*, 18(3), 275-290.

Schreft, Stacey L. (2007) Risks of Identity Theft: Can the Market Protect The Payment System, *Economic Review,* Vol. 92 Issue 4, pp5-40.

Scott, W. A. (1955). Reliability of content analysis: the case of nominal scale coding, *Public Opinion Quarterly,* XIX, 321-325.

Shareef, M. A., and Kumar, V. (2012). Prevent/Control Identity Theft: Impact on Trust and Consumers' Purchase Intention in B2C EC. *Information Resources Management Journal,* 25(3), 30-60.

Shelton, M. L. and Rogers, R. W. (1981). Fear-arousing and empathy-arousing appeals to help: The pathos of persuasion, *Journal of Applied Social Psychology*, 11, pp366-378.

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.

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.

Sproule, Susan and Archer, Norm (2008b). Measuring Identity Theft in Canada: 2008 Consumer Survey, McMaster eBusiness Research Centre (MeRC), Working Paper #23, July.

Stajano, Frank And Wilson, Paul (2011). Understanding Scam Victims: Seven Principles for Systems Security, *Communications of the ACM*, Vol. 54, Issue 3, pp70-75.

Statscan (2013). Internet use by individuals, by selected characteristics, Statistics Canada, http://www.statcan.gc.ca/tables-tableaux/sum-som/l01/cst01/comm35a-eng.htm accessed Feb 15, 2014.

Stech, Katy (2012) Burglary Triggers Medical Records Firm’s Collapse, *Wall Street Journal Blogs*, http://blogs.wsj.com/bankruptcy/2012/03/12/burglary-triggers-medical-records-firm's-collapse, accessed June 18, 2012.

Strauss, Anselm L., Corbin, Juliet M., (1998) "Basics of qualitative research : techniques and procedures for developing grounded theory", Thousand Oaks: Sage Publications.

Schwartz, Paul M. and Solove, Daniel J. (2013) Reconciling Personal Information in the United States and European Union, UC Berkeley Public Law Research Paper No. 2271442. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2271442 accessed 2 July 2013.

Tabachnick, B. and Fidell, L. (2006). *Using Multivariate Statistics*. Boston: Allyn and Bacon.

Tanner Jr., J. F., Hunt, J. B., and Eppright, D. R. (1991). The Protection Motivation Model: A Normative Model of Fear Appeals. *Journal Of Marketing*, 55(3), 36-45.

Trafimow, D., Sheeran, P., Conner, M. and Finlay, K. A. (2002), Evidence that perceived behavioural control is a multidimensional construct: Perceived control and perceived difficulty. *British Journal of Social Psychology,* 41: 101–121.

Trope, Y., and Fishbach, A. (2000). Counteractive self-control in overcoming temptation, *Journal of Personality and Social Psychology,* 79(4), 493-506.

van der Velde., Frank W., Hooykaas, Christa and van der Pligt, Joop (1996). Conditional versus unconditional risk estimates in models of AIDS-related risk behaviour. *Psychology & Health*, *12*(1), pp87-100.

Webb, T. L., and Sheeran, P. (2006). Does Changing Behavioral Intentions Engender Behavior Change? A Meta-Analysis of the Experimental Evidence. *Psychological Bulletin*, 132(2), 249-268.

Weinstein, N. D. (1993). Testing four competing theories of health-protective behavior. *Health Psychology*, 12(4), pp324-333.

Weinstein, N. D., and Nicolich, M. (1993). Correct and incorrect interpretations of correlations between risk perceptions and risk behaviors. *Health Psychology*, 12(3), pp235-245.

Wolf, S., Gregory, W. L. and Stephan, W. G. (1986). Protection motivation theory: Prediction of intentions to engage in anti-nuclear war behaviors, *Journal of Applied Social Psychology*, 16, pp310-321.

Workman, M. (2009). How perceptions of justice affect security attitudes: Suggestions for practitioners and researchers. *Information Management & Computer Security*, 17(4), pp341-353.

Appendix A - Qualitative Instrument to Elicit Salient Beliefs

We are interested in your thoughts from three points of view: what you think, what others think and what factors have a bearing on what you do.

For example, suppose we were asking about your thoughts on eating a low-fat diet. Here are some questions similar to what we will ask and a sample participant's answers. The answers are shown in italics.

What do you think are the advantages of eating a low-fat diet?

Eating a low-fat diet makes me feel good about myself.
By eating a low-fat diet, I will reduce the risk of heart disease.
Eating a low-fat diet makes me feel healthier.
Eating a low-fat diet helps to maintain lower weight.

What do you think are the disadvantages of eating a low-fat diet?

Eating a low-fat diet means eating boring food.
Food that is low in fat does not taste good.
Eating a low-fat diet reduces my enjoyment of food.

What else comes to mind when you think about eating a low-fat diet?

Not eating a low-fat diet would make me feel guilty.

There might be individuals or groups that think you should or should not eat a low-fat diet. Please record relationships such as spouse, parents, boss, co-workers, or friends.

Please list the individuals or groups that would <u>approve</u> or that think you <u>should</u> eat a low-fat diet.

Health experts think I should eat a low-fat diet.
My parents think I should eat a low-fat diet.
People who report in the media think I should eat a low-fat diet.

Please list the individuals or groups that <u>disapprove</u> or think you <u>should not</u> eat a low-fat diet.

My family thinks I should not eat a low-fat diet.

Sometimes, when we are not sure what to do we look to see what others are doing. Please list the individuals or groups who are <u>most likely</u> to eat a low-fat diet.

My spouse eats a low-fat diet.

Please list the individuals or groups who are least likely to eat a low-fat diet.

My friends do not eat a low-fat diet.

Sometimes there are factors or circumstances that either help or hinder doing what we want to do.

List the factors or circumstances that would make it easy or enable you to eat a low-fat diet.

I would eat more low-fat food if it was readily available.

List the factors or circumstances that would make it difficult to eat or prevent you from eating a low-fat diet.

Eating a low-fat diet takes too much time.
Eating a low-fat diet costs too much money.
I find it hard to resist foods that are high in fat.
To eat a low-fat diet requires strong motivation.
High-fat foods are convenient.
I don't always know which foods are low in fat.

Now to the topic of this research, which is the prevention of consumer identity theft and fraud. Please take a few minutes to think about the possibility of someone stealing your personal identity information (birth date, credit card number, bank account number, social insurance number etc.) and what you might do to prevent the loss of such information. For each question, please list the thoughts that immediately come to mind. There are no right or wrong answers. We are only interested in your personal opinions. Please write each thought on a separate line.

1. What do you think are the advantages of protecting your personal identity information?

2. What do you think are the disadvantages of protecting your personal identity information?

3. What else comes to mind when you think about protecting your personal identity information?

There might be individuals or groups that think you should or should not protect your personal identity information. These might include your spouse, parents, relatives, boss, co-workers, or friends.

4. Please list the individuals or groups that would approve or that think you should protect your personal identity information.

5. Please list the individuals or groups that might disapprove or think you do not need to protect your personal identity information.

Sometimes, when we are not sure what to do, we look to see what others are doing.

6. Please list the individuals or groups who are most likely to protect their personal identity information.

7. Please list the individuals or groups who are least likely to protect their personal identity information.

Sometimes there are factors or circumstances that either help or hinder doing what we want to do.

8. List the factors or circumstances that would make it easy or enable you to protect your personal identity information.

9. List the factors or circumstances that would make it difficult for you to protect or prevent you from protecting your personal identity information.

These are questions about specific things you can and may already do to prevent identity theft and detect identity fraud.

Each of the following questions deals with an action or set of actions that may affect the chances of theft of your personal identity information or may help you detect if it has been misused. In your answers, please think about the advantages of doing the action(s), disadvantages of doing the action(s), factors that would help you do the action(s), factors that would hinder you from doing the action(s), and any other thoughts about doing the action(s).

10. Financial or sensitive documents may be physically secured (stored in a secure location such as a locked drawer or box, shredded before discarding, protected in a locked mailbox, etc.).

What do you think are the advantages, disadvantages, and factors that help or hinder securing your financial or sensitive documents?

11. Some passwords may be more secure than others (using different passwords for different applications or services, including special characters and numbers in passwords, and using hard-to-break passwords; that is, not using family members' names or common dictionary words).

What do you think are the advantages, disadvantages, and factors that help or hinder using secure passwords?

12. By law, credit agencies (Equifax and TransUnion in Canada) must provide a free copy of your credit report on written request.

What do you think are the advantages, disadvantages, and factors that help or hinder your requesting a copy of your credit report?

13. What do you think are the advantages, disadvantages, and factors that help or hinder your monitoring the activity on your credit card(s) and/or bank account(s)?

14. What do you think are the advantages, disadvantages, and factors that help or hinder your using “remember my card number” or "remember my password” for online log-ins?

15. What do you think are the advantages, disadvantages, and factors that help or hinder giving personal information over the phone to people who do surveys, or people offering products or services at special prices?

16. What do you think are the advantages, disadvantages, and factors that help or hinder responding to a business e-mail inquiry by clicking on a link in an e-mail?

17a. Do You own your own home?

Yes
No

[If the answer to 17a is Yes then administer question 17b. Otherwise skip question 17b.]

17b. What do you think are the advantages, disadvantages, and factors that help or hinder checking the Land Registry Office records to ensure validity of your home ownership?

The following questions make use of rating scales with 7 places; you are to select the option that best describes your opinion.

For example, if you were asked to rate "The Weather in Canada" on such a scale the 7 places might be as follows:

The Weather in Canada is:

extremely bad
quite bad
slightly bad
neither bad nor good
slightly good
quite good
extremely good

If you think the weather in Canada is extremely good, then you would select the last option.
If you think the weather in Canada is quite bad, then you would select the second option.
If you think the weather in Canada is neither good nor bad, then you would select the middle option.

18. If I took no precautions to prevent it, the chances of my personal identity information being stolen are:

- extremely unlikely
- quite unlikely
- slightly unlikely
- neither unlikely nor likely
- slightly likely
- quite likely
- extremely likely

19. If my personal identity information were to be stolen, the consequences to me would be:

- extremely minor
- quite minor
- slightly minor
- neither minor nor serious
- slightly serious
- quite serious
- extremely serious

20. Protecting my personal identity information is:

- extremely easy
- quite easy
- slightly easy
- neither easy nor difficult
- slightly difficult
- quite difficult
- extremely difficult

21 I am ________ with the precautions I currently take to prevent theft of my personal identity information.

- extremely unsatisfied
- quite unsatisfied
- slightly unsatisfied
- neither unsatisfied nor satisfied
- slightly satisfied
- quite satisfied
- extremely satisfied

22. I am _________ that I can detect the fraudulent use of my personal identity information in a timely fashion.

- extremely unsure
- quite unsure
- slightly unsure
- neither unsure nor confident
- slightly confident
- quite confident
- extremely confident Choose one of the following answers

23a. Has your credit card information ever been used fraudulently?
Choose one of the following answers

Yes
No

[If the answer to 23a is Yes then administer question 23b. Otherwise skip question 23b.]

23b. Did it happen within the last year?
Choose one of the following answers
Yes
No

24a. Have you ever experienced any other kind of identity fraud?
Choose one of the following answers

Yes
No
[If the answer to 24a is Yes then administer question 24b. Otherwise skip question 24b.]

24b. Did it happen within the last year?
Choose one of the following answers

Yes
No

Thank you so much for your assistance with this research.

Appendix B – Results of Phase 1 Exploratory Survey

Salient Belief Class	Code	Freq in All Segments	Keep
General Outcome	GO01-Avoid financial loss	21	Yes
	GO03-Thwarts criminal activity	19	Yes
	GO07-Personal & information privacy	17	Yes
	GO08-Peace of mind	17	Yes
	GO05-Avoids hassle of dealing with fraud	12	Yes
	GO02-Complicates transactions	10	Yes
	GO06-Information security	9	Yes
	GO04-Prevents loss of reputation	6	Yes
	GO10-Lack of visibility to legitimate users	4	Yes
	GO11-It will not happen to me	3	No
General Outcome		**118**	
General Subjective Norm	SN08-Financial institutions	29	Yes
	SN05-Friends	23	Yes
	SN09-Government	20	Yes
	SN07-Co-workers	18	Yes
	SN13-Youth	18	Yes
	SN04-Siblings	17	Yes
	SN01-Spouse	16	Yes
	SN10-High net worth individuals	12	Yes
	SN12-Seniors	12	Yes
	SN17-Criminals	12	Yes
	SN02-Children	10	Yes
	SN21-The uninformed or unthinking	10	No
	SN03-Parents	9	Yes
	SN15-Retailers	8	No
	SN19-Low net worth people	8	No
	SN16-Health care providers	4	No
	SN18-Previous victims	4	No

	SN20-Technological luddites	3	No
General Social Norm		**233**	
General Control	GX01-Taking too much time and effort	22	Yes
	GH02-Up to date information/training/tutorial	15	Yes
	GH11-Better security on bank machines and retail checkout	14	No
	GH04-Personal diligence/engagement	11	Yes
	GH03-Business requiring only needed info	10	No
	GX02-Costs too much	9	Yes
	GH10-Security software/service	7	No
	GH06-More flexible payment options	6	No
	GX04-New technology/new ways of victimization	6	No
	GH13-Business that fail to protect information	5	No
	GH07-Better security on web sites (particularly social sites)	4	No
	GH09-I can't control what business/government does with my info	4	No
	GH01-"Hack-proof" computer	3	No
	GH12-Limiting the documents I carry	3	No
	GH14-Physical security at ATM/retailer - shielding PINs etc.	3	No
	GX05-Default web site security settings too low	3	No
	GH08-Everyone is vulnerable	2	No
	GX06-Inadequate law-local and in other jurisdictions	2	No
	GX07-Non-secured communications (online, phone, snail-mail)	2	No
	GH05-Bills/invoices without complete ID info	1	No
General Control		**132**	
Physical Security Outcome	PSO1-Security	9	Yes
	PSO4-Under personal control	9	Yes
	PSO2-Loss of identity information	4	Yes
	PSO3-Info available for taxes etc.	1	No
Physical Security Outcome		**23**	
Physical Security Control	PSX2-Time consuming & inconvenient	20	Yes
	PSH1-Access to shredder	13	Yes
	PSX1-Additional Cost	9	Yes
	PSX5-Requires discipline	9	Yes

	PSH2-Access to secure location	8	Yes
	PSX3-Secure place may not be secure (fire etc.)	8	No
Physical Security Control		**67**	
Password Outcome	PWO1-Secure passwords reduce risk of ID crime	14	Yes
	PWO2-Using different passwords reduces risk	7	Yes
	PWO3-Elaborate password protocols slow access	2	Yes
	PWO4-Passwords provide false sense of security	2	Yes
	PWO6-Forgetting password and re-establishing access is a 'hassle'	2	Yes
	PWO5-Passwords are not needed-site can ask personal info	1	No
Password Outcome		**28**	
Password Control	PWX1-Too many passwords for different apps	22	Yes
	PWX2-Secure passwords are hard to remember	19	Yes
	PWH1-Secure place to record passwords	14	Yes
	PWX4-Differing password standards	9	Yes
	PWX5-Frequent password changes are hard to remember	6	Yes
	PWH2-Knowledge of how to build secure password	4	Yes
	PWH3-Sites that enforce password standards	4	No
	PWH4-Reminders to change password	1	No
	PWX7-Need to remember client/account/etc. # as well as password	1	No
Password Control		**80**	
Credit Report Outcome	CRO3-Good to know that it is correct and where I stand	16	Yes
	CRO1-Detects unauthorized use	7	Yes
	CRO2-Provides no benefit	6	Yes
Credit Report Outcome		**29**	
Credit Report Control	CRH1-Knowledge/awareness of process	8	Yes
	CRX1-Time consuming	7	Yes
	CRX2-Process is not easy	7	Yes
	CRX3-Security of report (in mail - subject to interception)	3	Yes
	CRH2-Online access	2	Yes
Credit Report Control		**27**	
Monitor Accounts Outcome	MAO1-Detects unauthorized activity	20	Yes
	MAO2-Monitoring by banks makes monitoring less critical	6	Yes

Monitor Accounts Outcome		**26**	
Monitor Accounts Control	MAX1-Requires too much time and effort	9	Yes
	MAX2-Banking info on computer vulnerable to 'hackers'	5	Yes
	MAH1-Ease of use	4	Yes
	MAH2-Regular statements	3	Yes
	MAX3-Elaborate online security protocols	3	Yes
	MAX4-Hard to monitor joint accounts	2	Yes
	MAX5-Dealing with multiple institutions	1	No
	MAX6-Not always up to date	1	No
Monitor Accounts Control		**28**	
Remember Password Outcome	RMO1-Passwords vulnerable to 'hackers'	24	Yes
	RMO3-Easy and convenient	11	Yes
	RMO2-Don't need to write down or remember passwords	10	Yes
	RMO4-'Logon' password protects against unauthorized use	1	No
Remember Password Outcome		**46**	
Remember Password Control	RMH2-Secure passwords are hard to remember	6	Yes
	RMX1-Factor - is computer used by others	5	Yes
	RMH1-Capability is typically available	2	Yes
	RMX2-'Remember' does not always work	1	Yes
Remember Password Control		**14**	
Phone Info Outcome	PHO1-Leave yourself open to crime-don't know who you are talking to	19	Yes
	PHO2-Info may be used for other purposes	8	Yes
	PHO5-Phone interaction is easy and convenient	4	Yes
	PHO3-Surveys provide no benefit to me	2	Yes
	PHO4-Better prices are available over the phone	2	Yes
	PHO6-I get no record of interaction	2	Yes
Phone Info Outcome		**37**	
Phone Info Control	PHH1-Knowing the identity of the caller	6	Yes
	PHX1-They always call back	3	Yes
	PHX2-Takes too much time	3	Yes
	PHX3-Caller determines the timing - intrusive	3	No
Phone Info Control		**15**	

Click Link Outcome	CLO1-Link could lead to virus, worm, other malware or id theft	25	Yes
	CLO2-Easy and convenient	12	Yes
	CLO4-Sometimes get good deals	2	Yes
*	CLO3-Doing it once generates more e-mail	1	Yes
	CLO5-Allows info tailored to you	1	Yes
Click Link Outcome		**41**	
Click Link Control	CLH1-Knowing the identity of the sender	10	Yes
	CLH2-You can always close the link if it's not what you expected	2	Yes
Click Link Control		**12**	
Land Registry Outcome	LRO2-Peace of mind	11	Yes
	LRO5-Only needed when buying or selling home	6	Yes
	LRO3-Provides no benefit	4	Yes
	LRO1-Detect unauthorized mortgage or liens	3	Yes
	LRO4-Source of ID info to criminals	3	Yes
Land Registry Outcome		**27**	
Land Registry Control	LRH1-Knowing the procedure	11	Yes
	LRX1-Takes time and effort	5	Yes
	LRX2-Cost	3	Yes
Land Registry Control		**19**	
		1002	

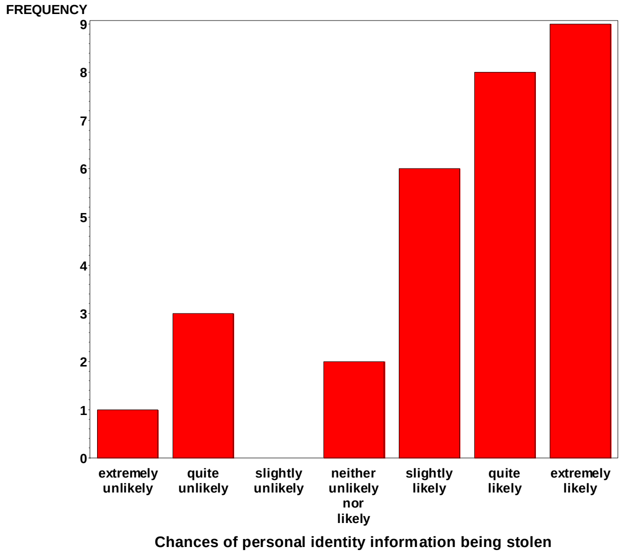
Inter-Rater Reliability

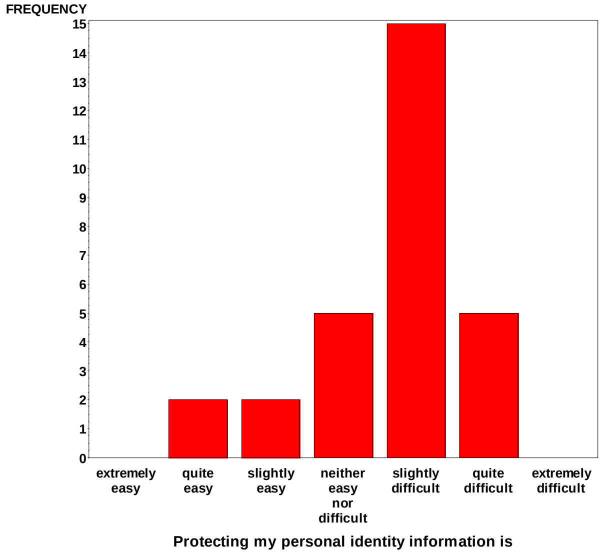
Statistic	Kappa[20]	Scott[21]	Gwet[22]	Brennan Prediger[23]
Coefficient	0.745	0.745	0.749	0.749
Standard Error	0.014	0.014	0.013	0.013
95% Lower Conf. Limit	0.718	0.718	0.724	0.724
95% Upper Conf. Limit	0.772	0.772	0.775	0.775
One-Sided P-Value	0.000	0.000	0.000	0.000
Two-Sided P-Value	0.000	0.000	0.000	0.000

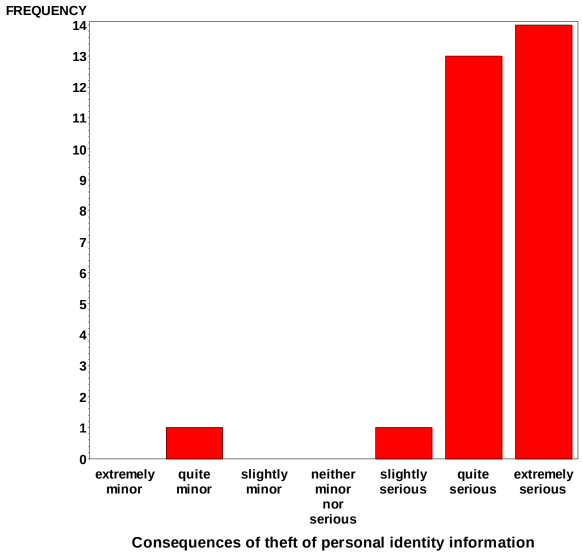
[20] Cohen, 1960
[21] Scott, 1955
[22] Gwet, 2008
[23] Brennan and Prediger, 1981

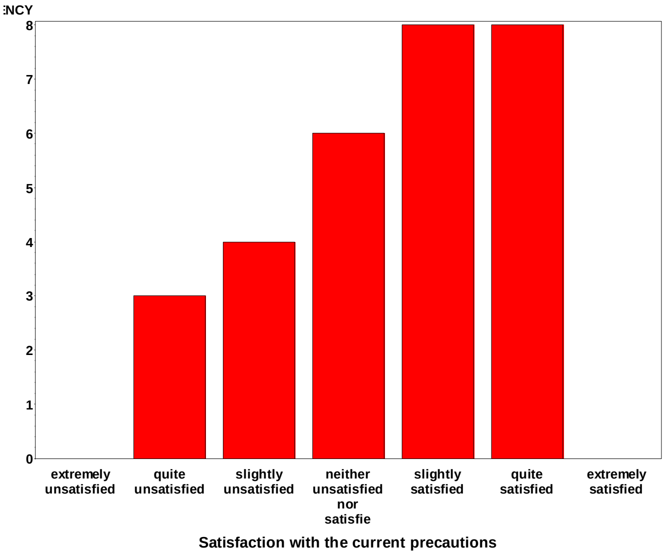
Appendix C – Quantitative Questions on Phase 1 Exploratory Survey

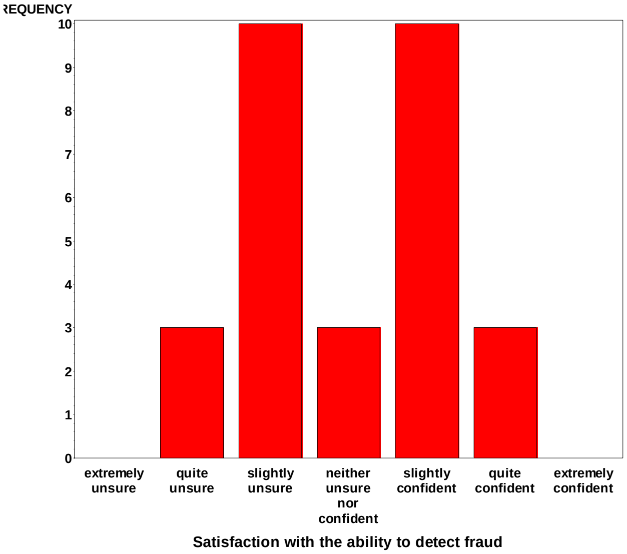
Attitudes



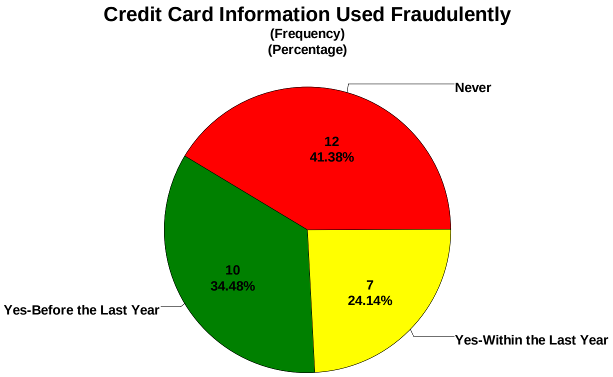


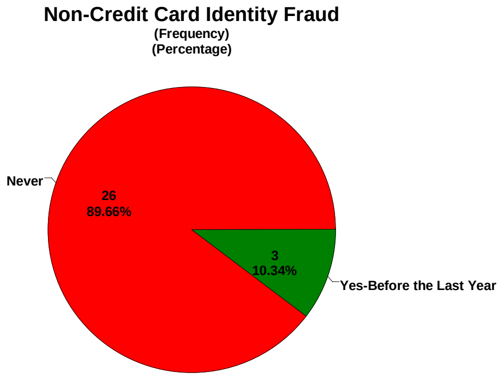





REQUENCY
10
9
8
7
6
5
4
3
2
1
0
extremely unsure
quite unsure
slightly unsure
neither unsure nor confident
slightly confident
quite confident
extremely confident
Satisfaction with the ability to detect fraud

Experience


Credit Card Information Used Fraudulently
(Frequency)
(Percentage)
Never
12
41.38%
10
34.48%
Yes-Before the Last Year
7
24.14%
Yes-Within the Last Year


Non-Credit Card Identity Fraud
(Frequency)
(Percentage)
Never
26
89.66%
3
10.34%
Yes-Before the Last Year

Appendix D – Quantitative Survey

Explanatory notes are in red.
Survey control instructions are in blue.
Scales are in green.

Identity Theft Prevention and Identity Fraud Detection

This survey is about identity theft and fraud. This research is part of a Ph.D. program at McMaster University. The objective of this study is to identify the motivations behind consumer behaviours that can prevent identity theft and fraud. Understanding the beliefs that predetermine these behaviours is key to providing better education and programs to assist consumers in minimizing the impact of identity theft and fraud.

The researchers involved in this study are:

John Gilbert Ph.D. Student
DeGroote School of Business
McMaster University
1280 Main St. West
Hamilton, ON L8S 4M4
Phone 905-525-9140 Ext. 26397
e-mail gilbeja2@mcmaster.ca

Norm Archer, Ph.D. Professor Emeritus
DeGroote School of Business
McMaster University
1280 Main St. West
Hamilton, ON L8S 4M4
Phone 905-525-9140 Ext. 23944
e-mail archer@mcmaster.ca

This online questionnaire that will take you about 30 minutes to complete. We hope to learn more about what you think about things you may do and things you can do to prevent identity theft and detect identity fraud.

It is unlikely that your participation in this study will cause any discomfort or harm. Some of the questions may cause you to reflect on issues or decisions that may be a source of concern or worry for you. Any responses you provide will be treated confidentially by researchers.

All information collected will be kept in strict confidence. Only the researchers named above will have access to the data. Participation is anonymous and participants will not be identified individually in any reports or analyses resulting from this research project.

It is important for you to know that any information you provide will be anonymous. The web site is programmed to collect responses only and will not collect any information that could potentially identify you (such as machine identifiers or IP addresses). Your contribution will also be confidential. The data collected from this study, with no personal identifiers, will be maintained on a password-protected computer database in a restricted access area of the University. As well, the data will be electronically archived after completion of the study, maintained for two years and then erased. If you have any questions or concerns about the anonymity or confidentiality of this study, please do not hesitate to contact either the faculty supervisor (Dr. Archer see above) or the McMaster Research Ethics Board (see below).

Participation in this study is voluntary. You do not have to participate and if you start, you may drop out of the questionnaire at any time. Since there is no way of knowing who participates, there can be no repercussions to you for not participating.

This study has been reviewed by the McMaster University Research Ethics Board and received ethics clearance. It contains all necessary confidentiality protocols with respect to using the internet for research purposes. If you have concerns or questions about your rights as a participant or about the way the study is conducted, please contact:

McMaster Research Ethics Secretariat
Telephone: (905) 525-9140 ext. 23142
c/o Research Office for Administrative Development and Support
E-mail: ethicsoffice@mcmaster.ca

As mentioned above, participation in this study is voluntary. You must be eighteen years or older to participate. Clicking on the 'next' button below to start this survey, signifies your agreement to participate in the study. If you start, you may drop out of the questionnaire at any time.

If with full knowledge of all the foregoing, and of your own free will you agree to participate in this study, please click on the 'next' button.

There are 60 questions in this survey

Initial Questions (Screening and demographic questions)

1 [S4] Are you? *

Please choose **only one** of the following:

Female
Male

2 [S5] Where do you live? *

Please choose **only one** of the following:

Newfoundland and Labrador
Prince Edward Island
Nova Scotia
New Brunswick

Ontario
Quebec
Manitoba
Saskatchewan
Alberta
British Columbia
Other

3 [S3] How old are you? *

Please choose **only one** of the following:

Under 18 years
18 to 25 years
26 to 35 years
36 to 45 years
46 to 55 years
56 to 65 years
66 to 75 years
Over 75 years

4 [S1]How many bank accounts do you have? *

Please choose **only one** of the following:

0
1
2
3
4
More than 4
Prefer not to answer

5 [S2]How many credit cards do you have? *

Please choose **only one** of the following:

0
1
2
3
4
More than 4
Prefer not to answer

6 [S6A]Have you ever been the victim of credit card fraud where someone made unauthorized charges to your credit card? *

Please choose **only one** of the following:

Yes
No

Only present this question if the following conditions are met:
° Answer was 'Yes' at question '6 [S6A]' (Have you ever been the victim of credit card fraud where someone made unauthorized charges to your credit card?)

7 [S6B]When did you experience credit card fraud (the latest time if more than once)? *

Please choose **only one** of the following:

last 3 months
4-6 months ago
7-12 months ago
1 year ago
2-4 years ago
5 or more years ago

8 [S7A]Have you ever been the victim of another kind of identity fraud (other than credit card)? *

Please choose **only one** of the following:

Yes
No

Only present this question if the following conditions are met:
° Answer was 'Yes' at question '8 [S7A]' (Have you ever been the victim of another kind of identity fraud (other than credit card)?)

9 [S7B]When did the other identity fraud happen (the latest time if more than once)? *

Please choose **only one** of the following:

last 3 months
4-6 months ago
7-12 months ago
1 year ago
2-4 years ago
5 or more years ago

General Questions 1 (Outcome evaluations of personal identity information protection)

10 [A]What do you believe? *

Please choose the appropriate response for each item:

Scale: extremely bad, quite bad, somewhat bad, neither bad nor good, somewhat good, quite good, extremely good

Avoiding financial loss is
Putting a stop to criminal activity is
Having peace of mind is
Protecting my personal and information privacy is
Complicated transactions are
Avoiding the hassle of dealing with fraud is
Securing my personal information is
Preventing the loss of my reputation is
Reducing my online visibility to legitimate users is

General Questions 2 (Self-reported behaviours. Includes behaviours for all 5 components)

11 [H]How often do you do the following things? *

Please choose the appropriate response for each item:

Scale: never, rarely, sometimes, half the time, often, usually, always

I Monitor credit card accounts and activity at least once a month
I monitor bank account balances and activity at least once a month
I request a copy of my credit report at least once a year
I check Land Registry Office records at least once a year to ensure validity of ownership
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 have different passwords for different applications or services
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 select "remember my card number" or "remember my password" for online log-ins
I give personal information over the phone to people who do surveys, or people offering products or services at special prices
I respond to a business by clicking on a link in an email

General Questions 3 (Direct measures of attitude, subjective norm, perceived behavioural control, and intention. Includes all five behavioural components)

12 [G]Please answer the following *

Please choose the appropriate response for each item:

Scale is 7 points with the extreme points indicated after the item.

Whether or not I click on a link in an e-mail is completely up to me: strongly disagree - strongly agree

For me to secure my financial documents is: extremely difficult - extremely easy

I will make an effort to monitor my bank account and credit card activity at least once a month: definitely will not - definitely will

For me to use ‘remember my password’ is: extremely bad - extremely good

I will make an effort to use ‘remember my password’: definitely will not - definitely will

For me to check my credit report at least once a year is: extremely bad - extremely good

I will make an effort to click on links in e-mails: definitely will not - definitely will

For me to secure my financial documents is: extremely worthless - extremely valuable

For me to monitor my bank account and credit card activity at least once a month is: extremely worthless - extremely valuable

For me to monitor my bank account and credit card activity at least once a month is: extremely bad - extremely good

I am confident that if I wanted to, I could secure my financial documents: definitely false - definitely true

Whether or not I give personal information over the phone is completely up to me: strongly disagree - strongly agree

I will make an effort to give personal information over the phone: definitely will not - definitely will

For me to give personal information over the phone is: extremely worthless - extremely valuable

Most people whose opinions I value, would approve of my protecting my personal identity information: strongly disagree - strongly agree

It is expected of me that I protect my personal identity information: definitely false - definitely true

I am confident that if I wanted to, I could use ‘remember my password’: definitely false - definitely true

For me to use secure passwords is:
extremely unpleasant - extremely pleasant

I plan to check my credit report at least once a year:
extremely unlikely - extremely likely

Whether or not I check my credit report at least once a year is completely up to me:
strongly disagree - strongly agree

I intend to use secure passwords:
strongly disagree - strongly agree

For me to monitor my bank account and credit card activity is:
extremely difficult - extremely easy

I intend to secure my financial documents:
strongly disagree - strongly agree

For me to click on a link in an e-mail is:
extremely boring - extremely interesting

For me to use secure passwords is:
extremely difficult - extremely easy

I will make an effort to check my credit report at least once a year:
definitely will not - definitely will

For me to secure my financial documents is:
extremely boring - extremely interesting

I plan to use ‘remember my password’:
extremely unlikely - extremely likely

For me to use secure passwords is:
extremely bad - extremely good

I plan to give personal information over the phone:
extremely unlikely - extremely likely

Most people who are important to me think that I ___ protect my personal identity information: definitely should not - definitely should

For me to secure my financial documents is:
extremely bad - extremely good

I plan to click on a links in e-mails:
extremely unlikely - extremely likely

I intend to give personal information over the phone:
strongly disagree - strongly agree

I will make an effort to secure my financial documents:
definitely will not - definitely will

Whether or not I use secure passwords is completely up to me:
strongly disagree - strongly agree

For me to give personal information over the phone is:
extremely boring - extremely interesting

For me to check my credit report at least once a year is:
extremely worthless - extremely valuable

I will make an effort to use secure passwords:
definitely will not - definitely will

Whether or not I secure my financial documents is completely up to me:
strongly disagree - strongly agree

For me to give personal information over the phone is:
extremely difficult - extremely easy

Whether of not I monitor my bank account and credit card activity at least once a month is completely up to me: strongly disagree - strongly agree

For me to click on a link in an e-mail is:
extremely difficult - extremely easy

For me to check my credit report at least once a year is:
extremely boring - extremely interesting

For me to use ‘remember my password’ is:
extremely difficult - extremely easy

Most of my friends protect their personal identity information:
definitely false - definitely true

I am confident that if I wanted to, I could give personal information over the phone:
definitely false - definitely true

For me to use ‘remember my password’ is:
extremely boring - extremely interesting

I am confident that if I wanted to, I could check my credit report at least once a year:
definitely false - definitely true

For me to give personal information over the phone is:
extremely bad - extremely good

I intend to use ‘remember my password’:
strongly disagree - strongly agree

I am confident that if I wanted to, I could monitor my bank account and credit card activity at least once a month: definitely false - definitely true

For me to click on a link in an e-mail is:
extremely worthless - extremely valuable

For me to click on a link in an e-mail is:
extremely bad - extremely good

For me to click on a link in an e-mail is:
extremely boring - extremely interesting

I plan to monitor my bank account and credit card activity at least once a month:
extremely unlikely - extremely likely

I plan to use secure passwords:
extremely unlikely - extremely likely

For me to use secure passwords is:
extremely worthless - extremely valuable

For me to monitor my bank account and credit card activity at least once a month is:
extremely unpleasant - extremely pleasant

I am confident that if I wanted to, I could use secure passwords:
definitely false - definitely true

I intend to monitor my bank account and credit card activity at least once a month:
strongly disagree - strongly agree

I am confident that if I wanted to, I could click on a link in an e-mail:
definitely false - definitely true

I intend to check my credit report at least once a year:
strongly disagree - strongly agree

I plan to secure my financial documents:
extremely unlikely - extremely likely

Whether or not I use ‘remember my password’ is completely up to me:
strongly disagree - strongly agree

For me to check my credit report at least once a year is:
extremely difficult - extremely easy

For me to use ‘remember my password’ is:
extremely worthless - extremely valuable

13 [HomeOwn]Do you own your home? *

Please choose **only one** of the following:

Yes
No

Only present this question if the following conditions are met:
° Answer was 'Yes' at question '13 [HomeOwn]' (Do you own your home?)

14 [Gb]Please answer the following *

Please choose the appropriate response for each item:

Scale is 7 points with the extreme points indicated after the item.

For me to check the land registry at least once a year is:
extremely bad - extremely good

I plan to check the land registry for my home at least once a year:
extremely unlikely - extremely likely

I am confident that if I wanted to, I could check the land registry at least once a year:
definitely false - definitely true

For me to check the land registry at least once a year is:
extremely difficult - extremely easy

Whether or not I check the land registry at least once a year is completely up to me:
strongly disagree - strongly agree

I intend to check the land registry at least once a year:
strongly disagree - strongly agree

I will make an effort to check the land registry at least once a year:
definitely will not - definitely will

For me to check the land registry at least once a year is:
extremely boring - quite interesting

For me to check the land registry at least once a year is:
extremely worthless - extremely valuable

General Questions 4 (Motivation to comply with normative beliefs)

15 [D]How much do you care about the opinions of others? *

Please choose the appropriate response for each item:

Scale: not at all, just a little, somewhat, moderately, a lot, quite a lot, very much, Not Applicable

Generally speaking, how much do you care what financial institutions (banks, investment counselor, financial advisor) think you should do
Generally speaking, how much do you care what government (justice system, police) thinks you should do
Generally speaking, how much do you care what your friends think you should do?
Generally speaking, how much do you care what your co-workers (boss, employer) think you should do?
Generally speaking, how much do you care what your spouse thinks you should do?
Generally speaking, how much do you care what your brothers and sisters think you should do?
Generally speaking, how much do you care what young people think you should do?
Generally speaking, how much do you care what seniors think you should do?
Generally speaking, how much do you care what your parents think you should do?
Generally speaking, how much do you care what high net worth individuals think you should do?
Generally speaking, how much do you care what your children think you should do?
Generally speaking, how much do you care what criminals think you should do?

General Questions 5 (Perceived likelihood of outcomes of personal identity information protection)

16 [B]What are the chances of these things happening? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, some- what unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely

If I protect my personal identity information, it is ___ that I will avoid financial loss
If I protect my personal identity information, it is ___ that I will not be the victim of identity theft or identity fraud
If I protect my personal identity information, it is ___ that I will have peace of mind
If I protect my personal identity information, it is ___ that my personal information will remain private
If I protect my personal identity information, it is ___ that my transactions will be more complicated
If I protect my personal identity information, it is ___ that I will avoid the hassle of dealing with identity theft or identity fraud
If I protect my personal identity information, it is ___ that my personal information will be secure
If I protect my personal identity information, it is ___ that my reputation will be damaged
If I protect my personal identity information, it is ___ that my online visibility to legitimate users will be reduced

General Questions 6 (Control beliefs about personal identity information protection)

17 [E]How true are these statements? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

I have enough time to do what I need to do
I can easily find information on how to protect my personal identity information
I have trouble engaging in tasks that I ought to do
I have enough money to do what I need to do

General Questions 7 (Power of control factors about personal identity information protection)

18 [F]How true are these statements when you protect your personal identity information? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

Protecting my personal identity information takes a lot of time
Protecting my personal identity information requires a lot of knowledge
Protecting my personal identity information requires diligence and engagement
Protecting my personal identity information costs a lot of money

General Questions 8 (Normative beliefs about personal information protection)

19 [C]What do others think you should do? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, some- what unlikely, neither unlikely nor likely, some- what likely, quite likely, extremely likely

Financial institutions (banks, investment counselor, financial advisor) think I should protect my personal identity information.
Government (justice system, police) think I should protect my personal identity information
My friends think I should protect my personal identity information
My co-workers (boss, employer, fellow students) think I should protect my personal identity information
Young people think I should protect my personal identity information
Seniors think I should protect my personal identity information
High net worth individuals think I should protect my personal identity information
Criminals think I should protect my personal identity information

20 [Cb]What does family think you should do? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, somewhat unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely, does not apply

My spouse thinks I should protect my personal identity information
My brothers and sisters think I should protect my personal identity information
My parents think I should protect my personal identity information
My children think I should protect my personal identity information

General Questions 9 (PMT questions)

21 [I]What do you think about the threat of identity theft and fraud? *

Please choose the appropriate response for each item:

Scale: strongly disagree, disagree, some- what disagree, neither disagree nor agree, some- what agree, agree, strongly agree

If I did nothing to prevent it, I would worry about identity theft

If I do nothing to prevent it, there is a good possibility that I will experience identity fraud

I know many people who have been victims of identity fraud

If they do nothing to prevent it, people in my circumstances are likely have their identities stolen

I worry less about credit card fraud than other identity fraud

If it happened to me, identity fraud would severely affect my life

Identity fraud is a serious problem

The threat of identity theft is too serious for me to ignore

Identity fraud is hard to recover from

Credit card fraud is much less serious than other identity fraud

Some people do not read the questions carefully or consider their answers thoughtfully. To indicate that you have read and answered the questions carefully and thoughtfully, please select 'neither disagree nor agree'

General Questions 10 (Qualitative questions)

22 [K01]In what ways do you think you are most vulnerable to identity theft?

Please write your answer here:

23 [K02]What do you think are the most important things you can do to prevent identity theft?

Please write your answer here:

24 [K03]What do you think are the most important things you can do to detect identity fraud?

Please write your answer here:

25 [RANDOM]

Generate a random selection of five alternatives: ‘physical’, ‘accounts’, ‘risky’, ‘agencies’ or ‘passwords’

Specific Questions 1 (Physical security outcomes)

Only present Specific Questions 1 if the following conditions are met:
° Answer at question 25 was 'physical'

26 [PSA]What do you think about these possibilities? *

Please choose the appropriate response for each item:

Scale: extremely bad, quite bad, somewhat bad, neither bad nor good, somewhat good, quite good, extremely good

Maintaining security of my personal financial documents is
Maintaining personal control of my personal information is
Having a physical record of my financial transactions is
Losing my personal identity information is

27 [PSC]How true are these statements? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

I have enough time to do what I need to do
I have convenient access to a shredder
I have enough money to meet my needs
I have trouble engaging in tasks that I ought to do
I have or can easily get convenient access to a secure location to store my financial and sensitive documents

Specific Questions 2 (Physical security likelihoods)

Only present Specific Questions 2 if the following conditions are met:
° Answer at question 25 was 'physical'

28 [PSH]Financial or sensitive documents may be physically secured (stored in a secure location such as a locked drawer or box, shredded before discarding, protected in a locked mailbox, etc.).

29 [PSB]If you secure your financial and sensitive documents, what are the chances? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, somewhat unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely

If I physically secure my documents, it is ___ that my personal identity information will be secure
If I physically secure my documents, it is ___ that I will maintain personal control of my identity information
If I physically secure my documents, it is ___ that I will have a physical record of my financial transactions
If I physically secure my documents, it is ___ that I will lose my personal identity information

30 [PSD]How true are these statements when you physically secure your financial and sensitive documents? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

Securing my documents takes too much time
Securing my documents requires a shredder
Securing my documents is expensive
Securing my documents requires discipline
Securing my documents requires a location that is secure from accidental damage (natural disasters such as fire) and unauthorized access

Specific Questions 3 (Password outcomes)

Only present Specific Questions 3 if the following conditions are met:
° Answer at question 25 was 'passwords'

31 [PWA]What do you believe? *

Please choose the appropriate response for each item:

Scale: extremely bad, quite bad, somewhat bad, neither bad nor good, somewhat good, quite good, extremely good

Being the victim of identity crime is
Reducing the risk of identity crime is
Fast online access is
Maintaining a sense of security is
Forgetting a password is

32 [PWC]How true are these statements? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

I have difficulty remembering all my passwords
I do not have a secure place to store my passwords
I can easily find information on how to make secure passwords

Specific Questions 4 (Password likelihoods)

Only present Specific Questions 4 if the following conditions are met:
° Answer at question 25 was 'passwords'

33 [PWH]Some passwords are more secure than others. For example, you may use different passwords for different applications or services. You may also use hard-to-break passwords, that is, not using family members' names or common dictionary words and include special characters and numbers. You may also change important passwords frequently.

34 [PWB]If you use secure passwords, what are the chances? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, somewhat unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely

If I do *not* use secure passwords, it is ___ that I will be the victim of identity crime
If I *do* use secure passwords, it is ___ that I will reduce the risk of identity crime
If I *do* use secure passwords, it is ___ that online access will be slower
If I *do* use secure passwords, it is ___ that I will have a sense of security
If I *do* use a secure password, it is ___ that I will forget it

35 [PWD]How true are these statements when you use secure passwords? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

Too many applications with different passwords makes it difficult to remember them all
Frequently changing my passwords makes them difficult to remember
Differing password standards in different applications make remembering passwords difficult
Secure passwords are hard to remember
A secure place to store my passwords would make using secure passwords easier
I need to know what a secure password is and how to make one

Specific Questions 5 (Monitor accounts outcomes)

Only present Specific Questions 5 if the following conditions are met:
° Answer at question 25 was 'accounts'

36 [MAA]What do you believe? *

Please choose the appropriate response for each item:

Scale: extremely bad, quite bad, somewhat bad, neither bad nor good, somewhat good, quite good, extremely good

Detecting the unauthorized use of my bank accounts and credit cards is
Having banking information stored on my computer is
Having the bank monitor my accounts and credit cards is

37 [MAC]How true are these statements? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

I have enough time to do what I need to do
Online security protocols are not an obstacle for me
I get regular bank and credit card statements

My bank accounts or credit cards are jointly owned
The process to monitor my bank accounts and credit cards is easy and uncomplicated

Specific Questions 6 (Monitor accounts likelihoods)

Only present Specific Questions 6 if the following conditions are met:
° Answer at question 25 was 'accounts'

38 [MAB]If you keep an eye on the activity in your bank accounts and credit card accounts, what are the chances? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, somewhat unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely

If I keep an eye on my accounts, it is ___ that I will detect the unauthorized use of my accounts
If I keep an eye on my accounts, it is ___ that banking information will be stored on my computer
If I *do not* keep an eye on my accounts it is ___ that the bank will do it

39 [MAD]How true are these statements when you keep an eye on the activity in your bank accounts and credit cards accounts? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

Keeping an eye on my accounts takes too much time
Keeping an eye on my accounts uses elaborate online security protocols
Keeping an eye on my accounts needs regular statements
Keeping an eye on my accounts is difficult if they are jointly owned
Keeping an eye on my accounts is easier if the process is uncomplicated

Specific Questions 7 (Monitor agencies outcomes)

Only present Specific questions 7 if the following conditions are met:
° Answer at question 25 was 'agencies'

40 [CRA]What do you believe? *

Please choose the appropriate response for each item:

Scale: extremely bad, quite bad, somewhat bad, neither bad nor good, somewhat good, quite good, extremely good

Knowing that my credit history is correct is
Detecting the unauthorized use of my credit information is
Having a sense of security is
Having confidential information stolen from the regular mail is

41 [CRC]How true are these statements? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

I can easily find out how to get my credit report
I am able to follow the process of getting my credit report
I have enough time to do what I need to

Specific Questions 8 (Monitor agencies likelihoods)

Only present Specific Questions 8 if the following conditions are met:
° Answer at question 25 was 'agencies'

42 [CRH]By law, the credit agencies (Equifax and TransUnion in Canada) must provide a free copy of your credit report on written request.

43 [CRB]If you request a credit report, what are the chances? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, somewhat unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely

If I request a credit report, it is ___ that I can correct mistakes in my credit history
If I request a credit report, it is ___ that I can detect the unauthorized use of my credit information
If I request a credit report, it is ___ that I will have a sense of security
If I request a credit report, it is ___ that the report will be stolen from the regular mail
If I request a credit report, it is ___ that I will get no benefit

44 [CRD]How true are these statements when you request a credit report? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

Getting a credit report requires knowledge of the process to request it
Getting a credit report is not an easy process
Getting a credit report is time consuming

Specific Questions 9 (Land registry outcomes)

Only present Specific Questions 9 if the following conditions are met:
° Answer at question 25 was 'agencies' *and* answer was 'Yes' at question 13 (Do you own your home?)

45 [LRA]What do you believe? *

Please choose the appropriate response for each item:

Scale: extremely bad, quite bad, somewhat bad, neither bad nor good, somewhat good, quite good, extremely good

Detecting an unauthorized mortgage on my property is
Having peace of mind is
Providing personal information to identity thieves is
Being overly cautious is

46 [LRC]How true are these statements? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

I have enough time to do the things I need to do
I know or can easily find the procedure for checking the Land Registry Office
I have enough money for my needs

Specific Questions 10 (Land registry likelihoods)

Only present Specific Questions 10 if the following conditions are met:
° Answer at question 25 was 'agencies' *and* answer was 'Yes' at question 13 (Do you own your home?)

47 [LRH]You can check the Land Registry Office records to make sure that your home ownership is valid

48 [LRB]If you check the Land Registry Office, what are the chances? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, somewhat unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely

If I check the Land Registry Office, it is ___ that I can detect any unauthorized mortgage on my property
If I check the Land Registry Office, it is ___ that I will have peace of mind
If I check the Land Registry Office, it is ___ that it is a source of information to identity thieves
If I check the Land Registry Office, it is ___ it is only needed when buying or selling the property
If I check the Land Registry Office, it is ___ that I will receive no benefit

49 [LRD]How true are these statements when you check the Land Registry Office? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

Checking the Land Registry Office is time consuming
Checking the Land Registry Office requires knowing the procedure
Checking with the Land Registry Office is costly

Specific Questions 11 (Risky behaviour outcomes)

Only present Specific Questions 11 if the following conditions are met:
° Answer at question 25 was 'risky'

50 [RBA]What do you believe? *

Please choose the appropriate response for each item:

Scale: extremely bad, quite bad, somewhat bad, neither bad nor good, somewhat good, quite good, extremely good

“Hackers” finding out my password is
Getting e-mail I do not want is
Having a record of my transactions is
Knowing who you are giving your personal information to is
Getting good deals is
Saving money is
Not having to remember or write down passwords is
Convenience is
Having information tailored to me is
Ease of use and convenience are
Computer viruses, worms or other malware are
Knowing how my personal information will be used is
Making web sites easy to use is

51 [RBC]How true are these statements? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

My computer is used by others
I can always tell if the identity of an e-mail sender is not what they claim it to be
I have enough time to do what I need to do
‘Remember my password’ usually works for me
If I click on a link in an e-mail, I can always close the link with no harm if it is not what I expected
I give personal information over the phone only if I make the call
I only click on a link in an e-mail if I know the identity of the sender
Most of the software I use has ‘remember my password’
I have trouble remembering all my passwords
If I do not give personal information over the phone, I will not lose anything

Specific Questions 12 (Risky behaviour likelihoods)

Only present Specific Questions 12 if the following conditions are met:
° Answer at question 25 was 'risky'

52 [RBH01]Many times software will offer to "remember my card number" or "remember my password" for online log-ins.

53 [RBB]If you use 'remember by password' or 'remember my account', what are the chances? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, somewhat unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely

If I use 'remember my password', it is ___ that "hackers" will find out my password
If I use 'remember my password', it is ___ that I will not need to remember or write down passwords
If I use 'remember my password', it is ___ that web sites are easier to use

54 [RBD]How true are these statements when you use 'remember by password' or 'remember my account'? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

'Remember my' account or password is less secure if other people use my computer
'Remember my' account or password is not always available
'Remember my' account or password does not always work
Good (secure) passwords are hard to remember

55 [RBH2]Sometimes people who do surveys, or offer products or services at special prices request personal information over the phone

56 [RBF]If you give personal information over the phone, what are the chances? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, somewhat unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely

If I give personal information over the phone, it is ___ that I do not really know who the person is
If I give personal information over the phone, it is ___ that the information will be used in ways other than I expect
If I give personal information over the phone, it is ___ that it is easy and convenient
If I give personal information over the phone, it is ___ that I will get a good deal
If I give personal information over the phone, it is ___ that I will have a record of the conversation

If I give personal information over the phone, it is ___ that I will receive no benefit

57 [RBH]How true are these statements when you give personal information over the phone? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

I give personal information over the phone, only if I know the identity of the person I am talking to
Doing business over the phone takes too much time
The caller usually calls back at a later time

58 [RBH3]Some businesses send e-mails with links in them. Clicking on the link should take you to their web site.

59 [RBK]If you click on a link in an e-mail, what are the chances? *

Please choose the appropriate response for each item:

Scale: extremely unlikely, quite unlikely, somewhat unlikely, neither unlikely nor likely, somewhat likely, quite likely, extremely likely

If I click on a link in an e-mail, it is ___ that I will be the victim of malware
If I click on a link in an e-mail, it is ___ that it is easy and convenient
If I click on a link in an e-mail, it is ___ that I will get a good deal
If I click on a link in an e-mail, it is ___ that I get information tailored to me
If I click on a link in an e-mail, it is ___ that I will get more e-mail from the same source

60 [RBJ]How true are these statements when you click on a link in an e-mail? *

Please choose the appropriate response for each item:

Scale: extremely false, quite false, somewhat false, neither false nor true, somewhat true, quite true, extremely true

Knowing the sender reduces the risk of clicking on a link in an e-mail
I will not be the victim of malware if I just open a web page, close it, and do nothing else
It is difficult to know the true identity of the sender of an e-mail with a link

Thank you so much for your assistance with this research.

Appendix E – Summary Demographics

Number Bank Accounts		
	Frequency	Percent
1	92	25.48
2	127	35.18
3	85	23.55
4	30	8.31
>4	27	7.48

Number Credit Cards		
	Frequency	Percent
1	96	26.59
2	110	30.47
3	72	19.94
4	44	12.19
>4	39	10.80

Age		
	Frequency	Percent
18-25	29	8.03
26-35	115	31.86
36-45	66	18.28
46-55	65	18.01
56-65	63	17.45
66-75	21	5.82
> 75	2	0.55

Language		
	Frequency	Percent
English	272	75.35
French	89	24.65

Gender		
	Frequency	Percent
Female	199	55.12
Male	162	44.88

Province		
	Frequency	Percent
Newfoundland	14	3.88
P.E.I.	1	0.28
Nova Scotia	16	4.43
New Brunswick	13	3.60
Ontario	143	39.61
Quebec	89	24.65
Manitoba	13	3.60
Saskatchewan	9	2.49
Alberta	35	9.70
British Columbia	28	7.76

Credit Card Victim		
	Frequency	Percent
No	256	70.91
Yes	105	29.09

Other ID Fraud Victim		
	Frequency	Percent
No	321	88.92
Yes	40	11.08

Appendix F – Comparison of Sample to Population Demographics

	Gender								Total			
	Female				Male							
	Population		Sample		Population		Sample		Population		Sample	
Age	#	%	#	%	#	%	#	%	#	%	#	%
18-25	1,511,005	5.99	21	5.82	1,583,792	6.28	8	2.22	3,094,797	12.27	29	8.03
26-35	2,140,424	8.48	69	19.11	2,167,269	8.59	46	12.74	4,307,693	17.07	115	31.86
36-45	2,571,190	10.19	32	8.86	2,619,192	10.38	34	9.42	5,190,382	20.57	66	18.28
46-55	2,444,452	9.69	27	7.48	2,400,676	9.51	38	10.53	4,845,128	19.20	65	18.01
56-65	1,807,521	7.16	39	10.80	1,772,303	7.02	24	6.65	3,579,824	14.19	63	17.45
> 65	2,381,345	9.44	11	3.05	1,831,492	7.26	12	3.32	4,212,837	16.70	23	6.37
Total	12,855,937	50.95	199	55.12	12,374,724	49.05	162	44.88	25,230,661	100.00	361	100.00

Appendix G – Combined Loadings and Cross-Loadings

Loadings shown in **bold** and cross-loadings non-bold.
Dropped items shown in red.

Attitudes

		Credit	Land	Monitor	Physical	Password	Click on	Info Over	Remember
		Report	Registry	Accounts	Security	Security	Link	Phone	Password
		Attitude	Attitude	Attitude	Attitude	Attitude	Attitude	Attitude	Attitude
G24	Check my credit report (good)	**0.794**	-0.003	0.107	-0.132	-0.116	-0.018	-0.123	-0.171
G27	Check my credit report (valuable)	**0.891**	0.115	-0.133	0.067	-0.012	0.019	-0.016	-0.020
G30	Check my credit report (interesting)	**0.825**	-0.121	0.041	0.055	0.125	-0.003	0.136	0.186
G15	Check land registry (good)	0.019	**0.841**	-0.134	0.132	-0.029	0.049	-0.070	0.032
G18	Check land registry (valuable)	0.071	**0.915**	-0.013	-0.009	-0.049	0.038	-0.036	-0.056
G21	Check land registry (interesting)	-0.096	**0.853**	0.146	-0.121	0.081	-0.089	0.108	0.029
G03	Monitor my accounts and cards (good)	-0.027	0.149	**0.873**	-0.131	-0.064	-0.024	0.078	-0.234
G07	Monitor bank account/cards (valuable)	0.062	-0.035	**0.877**	0.062	-0.156	0.121	-0.119	0.196
G10	Monitor bank account/cards (interesting)	-0.064	-0.208	**0.476**	0.126	0.404	-0.178	0.077	0.067
G42	Secure my financial documents (good)	0.006	0.015	-0.059	**0.798**	0.096	0.005	0.005	-0.108
G45	Secure my financial documents (valuable)	0.258	0.021	0.055	**0.768**	-0.170	0.191	0.017	-0.029
G48	Secure my financial documents (interesting)	-0.304	-0.042	0.007	**0.667**	0.081	-0.225	-0.025	0.163
G33	Use secure passwords (good)	0.036	0.044	-0.042	0.053	**0.813**	0.131	-0.014	-0.075
G36	Use secure passwords (valuable)	0.176	-0.055	-0.071	-0.107	**0.805**	-0.019	0.076	0.173
G38	Use secure passwords (pleasant)	-0.261	0.012	0.139	0.065	**0.657**	-0.139	-0.075	-0.119
G60	Click on a link in an e-mail (good)	-0.094	0.017	0.082	-0.031	-0.035	**0.887**	-0.005	-0.035
G63	Click on a link in an e-mail (valuable)	-0.020	0.101	0.034	-0.006	-0.004	**0.924**	0.039	0.022
G66	Click on a link in an e-mail (interesting)	0.130	-0.138	-0.134	0.043	0.044	**0.783**	-0.041	0.014
G69	Give personal info over phone (good)	-0.222	-0.096	0.037	-0.043	0.098	0.117	**0.823**	0.014
G72	Give personal info over phone (valuable)	0.125	-0.126	0.057	0.043	-0.110	-0.538	**0.723**	0.039
G75	Give personal info over phone (interesting)	0.113	0.207	-0.087	0.006	-0.001	0.357	**0.820**	-0.049
G51	Use "remember my password" (good)	-0.325	0.004	0.005	-0.096	0.203	-0.193	0.162	**0.714**
G54	Use "remember my password" (valuable)	0.131	-0.047	0.030	0.049	-0.114	-0.019	-0.128	**0.842**
G57	Use "remember my password" (interesting)	0.150	0.045	-0.036	0.034	-0.060	0.190	-0.009	**0.814**
G02	Most important people think I should	-0.246	0.197	-0.048	-0.065	-0.010	0.055	0.031	0.045
G06	Friends protect their personal info	-0.467	-0.091	0.090	-0.144	0.207	0.161	-0.030	0.185
G09	Expected that I protect personal info	0.167	0.137	0.024	0.100	0.019	-0.218	-0.010	-0.071
G12	Most approve protecting personal info	0.351	-0.292	-0.023	0.048	-0.124	0.070	-0.006	-0.079
G23	Check my credit report (easy)	-0.219	-0.048	-0.119	0.059	0.072	-0.093	0.112	0.042
G26	Checking my credit report is up to me	-0.036	0.156	0.127	-0.019	0.042	-0.016	0.010	-0.118
G28	If wanted, could check my credit report	0.211	-0.091	-0.009	-0.033	-0.095	0.090	-0.101	0.064
G14	Check land registry (easy)	-0.255	-0.030	0.030	0.139	0.064	-0.017	0.100	-0.071
G17	Check land registry up to me	0.229	0.001	0.051	-0.228	0.011	-0.066	-0.174	0.165
G19	If wanted could check land registry	0.033	0.025	-0.068	0.067	-0.065	0.070	0.056	-0.075
G01	Monitor my accounts and cards (easy)	-0.405	0.278	0.054	0.160	0.012	-0.024	0.180	-0.121
G05	If I monitor accounts/cards is up to me	0.397	-0.075	0.041	-0.081	-0.071	-0.094	-0.084	0.013
G08	If I wanted to I could monitor accounts	-0.053	-0.159	-0.087	-0.055	0.060	0.113	-0.069	0.088
G41	Secure my financial documents (easy)	-0.083	-0.034	-0.223	0.351	0.071	0.033	0.052	0.035
G44	Whether I secure documents is up to me	0.308	-0.118	-0.102	-0.050	-0.098	-0.008	0.066	0.046
G46	If I wanted to, I could secure documents	-0.213	0.140	0.293	-0.265	0.028	-0.022	-0.108	-0.074
G32	Use secure passwords (easy)	-0.216	-0.089	-0.105	0.095	0.269	0.271	-0.041	0.025
G35	Whether use secure passwords is up to me	0.369	-0.043	0.020	0.014	-0.337	-0.075	0.155	-0.206
G37	If wanted, could use secure passwords	-0.123	0.114	0.075	-0.095	0.049	-0.173	-0.095	0.151
G59	Click on a link in an e-mail (easy)	0.148	0.035	-0.115	-0.058	0.026	0.081	0.259	0.085

G62	Click on a link in an e-mail is up to me	-0.006	0.000	0.288	0.127	-0.095	-0.345	0.039	-0.371
G64	If wanted could click on link in e-mail	-0.144	-0.034	0.052	0.031	-0.006	-0.007	-0.263	-0.006
G68	Giving personal info over phone (easy)	0.052	0.151	-0.147	-0.208	0.052	0.055	0.350	-0.046
G71	Give personal info over phone up to me	-0.127	-0.101	0.700	0.038	-0.167	-0.080	0.002	-0.324
G73	If wanted, give personal info over phone	-0.018	-0.118	-0.031	0.186	-0.009	-0.032	-0.328	0.122
G50	Use "remember my password" (easy)	0.016	0.271	-0.159	-0.094	0.080	-0.039	0.305	0.325
G53	Whether use "remember password" up to me	-0.042	0.014	-0.032	0.089	-0.176	-0.059	0.011	-0.217
G55	If wanted could use "remember password"	0.010	-0.238	0.154	0.029	0.031	0.066	-0.266	-0.154
G25	Plan to check my credit report	-0.080	0.022	0.047	0.040	-0.033	0.046	-0.025	-0.036
G29	Make an effort to check my credit report	-0.029	0.021	-0.038	0.012	0.046	0.049	0.017	-0.012
G31	Intend to check my credit report	0.113	-0.045	-0.009	-0.053	-0.014	-0.099	0.008	0.050
G16	Plan to check the land registry	-0.001	0.039	-0.017	0.038	-0.058	0.055	0.036	0.008
G20	Make effort to check land registry	0.022	0.012	0.025	0.005	0.018	0.006	-0.058	-0.004
G22	Intend to check land registry	-0.021	-0.049	-0.009	-0.041	0.038	-0.059	0.023	-0.004
G04	Plan to monitor my accounts and cards	0.064	-0.003	-0.044	-0.089	-0.033	0.009	0.018	0.054
G11	Make effort to monitor accounts/cards	0.041	-0.084	0.104	0.081	-0.014	0.011	-0.032	-0.075
G13	Intend to monitor my accounts and cards	-0.099	0.076	-0.047	0.018	0.045	-0.019	0.011	0.012
G43	Plan to secure my financial documents	-0.021	0.078	-0.045	-0.059	-0.065	0.012	0.034	-0.041
G47	Make an effort to secure documents	0.019	-0.062	-0.034	-0.080	0.130	-0.014	0.015	0.071
G49	Intend to secure my financial documents	0.002	-0.016	0.080	0.141	-0.066	0.001	-0.050	-0.031
G34	Plan to use secure passwords	-0.043	-0.060	-0.018	-0.042	0.063	-0.045	-0.038	0.227
G39	Make an effort to use secure passwords	0.130	0.026	0.022	-0.072	-0.014	-0.060	0.112	-0.022
G40	Intend to use secure passwords	-0.093	0.036	-0.005	0.122	-0.052	0.112	-0.079	-0.220
G61	Plan to click on links in e-mails	0.167	-0.087	-0.060	-0.030	0.027	0.198	-0.102	-0.046
G65	Make an effort to click on links	-0.111	0.142	0.103	-0.141	-0.016	-0.545	0.218	0.153
G67	Intend to click on links in e-mails	-0.067	-0.046	-0.036	0.165	-0.012	0.316	-0.103	-0.098
G70	Plan to give personal info over phone	-0.148	0.034	0.020	0.019	-0.019	0.077	0.045	-0.059
G74	Make effort-give personal inf over phone	0.204	0.020	0.100	0.005	-0.095	-0.187	-0.106	0.122
G76	Intend to give personal infor over phone	-0.034	-0.052	-0.109	-0.023	0.104	0.090	0.050	-0.050
G52	Plan to use "remember my password"	0.015	0.048	-0.035	0.068	-0.031	0.059	-0.043	-0.046
G56	Make effort to use "remember password"	-0.099	0.071	0.092	-0.095	0.093	-0.310	0.197	0.056
G58	Intend to use "remember my password"	0.074	-0.113	-0.048	0.017	-0.053	0.221	-0.135	-0.004
H01	Monitor credit card accounts	0.011	-0.017	0.054	-0.039	-0.014	0.021	-0.034	-0.005
H02	Monitor bank account balances	-0.011	0.017	-0.054	0.039	0.014	-0.021	0.034	0.005
H03	Request a copy of my credit report	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H04	Check land registry office records	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H07	Use a locked mailbox for incoming mail	0.164	-0.012	0.011	-0.252	0.010	0.033	-0.082	-0.398
H08	Shred financial or important documents	-0.101	0.140	0.025	0.246	-0.034	-0.104	0.112	0.050
H09	Keep financial info in secure place	-0.017	-0.125	-0.032	-0.060	0.026	0.076	-0.050	0.228
H05	Use hard-to-break passwords	0.140	-0.031	0.129	-0.052	-0.015	0.060	-0.116	-0.151
H06	Have different passwords	-0.140	0.031	-0.129	0.052	0.015	-0.060	0.116	0.151
H12	Click on link in e-mail	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H10	Use "remember my password"	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H11	Give personal information over the phone	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
I01	Worry about identity theft	0.140	-0.135	-0.022	0.145	-0.140	-0.034	-0.142	-0.024
I02	Good possibility I will be a victim	0.028	0.015	0.073	-0.137	0.086	-0.068	0.062	-0.004
I03	Know many people who have been victims	-0.056	-0.096	-0.098	0.167	0.115	0.056	0.061	0.190
I04	People like me are likely to be victims	-0.121	0.181	0.015	-0.116	-0.039	0.063	0.027	-0.109
I06	Identity fraud would severely affect	0.047	0.103	-0.138	0.203	-0.060	-0.228	0.011	0.092
I07	Identity fraud is a serious problem	-0.081	-0.025	0.198	-0.169	0.077	-0.008	0.083	-0.218
I08	Threat is too serious to ignore	0.001	-0.068	-0.015	-0.023	-0.036	0.184	0.014	-0.012
I09	Identity fraud is hard to recover from	0.034	-0.007	-0.046	-0.008	0.019	0.041	-0.107	0.137

Subjective Norm and Perceived Behavioural Control

		Subjective Norm	Credit Report PBC	Land Registry PBC	Monitor Accounts PBC	Physical Security PBC	Password Security PBC	Click on Link PBC	Info Over Phone PBC
G24	Check my credit report (good)	0.132	0.102	-0.051	-0.193	-0.055	0.037	0.094	-0.059
G27	Check my credit report (valuable)	-0.026	-0.051	-0.016	0.261	0.011	-0.123	-0.064	0.073
G30	Check my credit report (interesting)	-0.099	-0.043	0.067	-0.096	0.041	0.097	-0.021	-0.022
G15	Check land registry (good)	-0.112	0.082	0.008	0.152	-0.011	-0.049	0.034	-0.054
G18	Check land registry (valuable)	0.053	-0.017	-0.079	-0.036	0.002	-0.017	-0.002	0.056
G21	Check land registry (interesting)	0.053	-0.063	0.076	-0.111	0.009	0.066	-0.031	-0.007
G03	Monitor my accounts and cards (good)	0.099	-0.011	0.028	0.012	0.031	-0.180	0.027	0.067
G07	Monitor bank account/cards (valuable)	-0.007	0.084	-0.086	-0.023	0.034	-0.079	0.052	-0.030
G10	Monitor bank account/cards (interesting)	-0.169	-0.134	0.107	0.020	-0.118	0.475	-0.146	-0.069
G42	Secure my financial documents (good)	0.086	0.093	0.012	0.302	-0.153	-0.112	0.180	-0.100
G45	Secure my financial documents (valuable)	-0.063	-0.020	-0.230	-0.050	0.247	-0.176	-0.080	0.052
G48	Secure my financial documents (interesting)	-0.030	-0.088	0.250	-0.304	-0.101	0.336	-0.123	0.060
G33	Use secure passwords (good)	-0.081	0.091	-0.116	0.126	0.110	-0.096	0.034	-0.074
G36	Use secure passwords (valuable)	0.018	-0.123	0.063	0.222	-0.033	-0.118	0.057	0.075
G38	Use secure passwords (pleasant)	0.079	0.038	0.066	-0.428	-0.096	0.263	-0.111	0.000
G60	Click on a link in an e-mail (good)	-0.071	0.042	-0.066	-0.088	0.035	0.043	-0.060	0.062
G63	Click on a link in an e-mail (valuable)	0.014	-0.032	-0.030	0.052	0.008	-0.064	0.037	0.002
G66	Click on a link in an e-mail (interesting)	0.064	-0.010	0.110	0.039	-0.048	0.026	0.024	-0.073
G69	Give personal info over phone (good)	-0.163	0.070	-0.097	-0.111	0.138	-0.016	-0.068	0.104
G72	Give personal info over phone (valuable)	0.094	-0.077	0.078	0.070	-0.060	0.055	0.038	-0.201
G75	Give personal info over phone (interesting)	0.081	-0.003	0.029	0.049	-0.085	-0.033	0.034	0.073
G51	Use "remember my password" (good)	-0.112	0.152	-0.001	0.200	0.018	-0.029	0.012	-0.094
G54	Use "remember my password" (valuable)	0.037	0.019	-0.005	-0.111	-0.079	0.044	0.033	-0.022
G57	Use "remember my password" (interesting)	0.060	-0.153	0.006	-0.060	0.066	-0.020	-0.045	0.105
G02	Most important people think I should	**0.825**	0.136	-0.117	0.054	-0.124	0.113	0.276	-0.241
G06	Friends protect their personal info	**0.439**	-0.208	0.314	-0.049	-0.043	-0.192	-0.320	0.219
G09	Expected that I protect personal info	**0.785**	-0.111	0.124	0.115	-0.065	-0.011	-0.116	0.053
G12	Most approve protecting personal info	**0.787**	0.083	-0.176	-0.144	0.219	0.000	0.005	0.077
G23	Check my credit report (easy)	-0.024	**0.676**	0.057	-0.060	-0.059	-0.061	-0.068	-0.104
G26	Checking my credit report is up to me	-0.005	**0.689**	-0.056	0.207	0.047	0.192	-0.093	-0.016
G28	If wanted, could check my credit report	0.024	**0.819**	0.000	-0.124	0.009	-0.111	0.134	0.099
G14	Check land registry (easy)	-0.005	0.024	**0.767**	-0.049	0.069	-0.020	0.001	0.004
G17	Check land registry up to me	0.039	0.072	**0.727**	0.093	-0.030	0.013	0.035	-0.120
G19	If wanted could check land registry	-0.028	-0.080	**0.880**	-0.033	-0.035	0.007	-0.030	0.096
G01	Monitor my accounts and cards (easy)	0.022	-0.065	-0.020	**0.697**	-0.099	0.009	-0.024	0.017
G05	If I monitor accounts/cards is up to me	-0.062	-0.071	-0.054	**0.822**	0.176	0.193	0.042	-0.088
G08	If I wanted to I could monitor accounts	0.043	0.126	0.071	**0.827**	-0.092	-0.200	-0.022	0.073
G41	Secure my financial documents (easy)	-0.185	-0.213	-0.118	-0.297	**0.647**	-0.246	0.086	0.018
G44	Whether I secure documents is up to me	-0.008	-0.047	0.080	0.611	**0.680**	0.344	-0.234	0.105
G46	If I wanted to, I could secure documents	0.171	0.232	0.029	-0.305	**0.730**	-0.103	0.141	-0.114
G32	Use secure passwords (easy)	0.047	0.179	0.077	-0.238	-0.202	**0.688**	-0.083	0.048
G35	Whether use secure passwords is up to me	-0.039	-0.194	0.034	0.249	0.220	**0.666**	-0.326	0.107
G37	If wanted, could use secure passwords	-0.009	0.007	-0.095	-0.002	-0.009	**0.790**	0.347	-0.132
G59	Click on a link in an e-mail (easy)	0.015	-0.005	-0.114	0.185	0.026	-0.196	**0.807**	0.177
G62	Click on a link in an e-mail is up to me	-0.062	0.331	0.089	-0.376	-0.150	0.579	**0.172**	-0.155
G64	If wanted could click on link in e-mail	-0.002	-0.065	0.093	-0.103	0.006	0.071	**0.821**	-0.142
G68	Giving personal info over phone (easy)	0.027	-0.016	-0.028	0.141	-0.075	-0.070	-0.164	**0.776**

G71	Give personal info over phone up to me	-0.024	0.397	0.053	0.008	-0.003	0.328	-0.018	**0.201**
G73	If wanted, give personal info over phone	-0.019	-0.081	0.014	-0.134	0.071	-0.013	0.158	**0.828**
G50	Use "remember my password" (easy)	0.033	-0.060	-0.152	0.274	0.081	-0.399	0.051	0.069
G53	Whether use "remember password" up to me	0.121	-0.123	0.202	0.271	-0.062	0.419	0.112	-0.256
G55	If wanted could use "remember password"	-0.096	0.121	0.015	-0.387	-0.034	0.103	-0.107	0.086
G25	Plan to check my credit report	0.060	0.011	-0.039	-0.118	0.055	-0.003	0.079	-0.027
G29	Make an effort to check my credit report	-0.051	-0.054	-0.008	0.152	-0.035	0.045	-0.063	0.012
G31	Intend to check my credit report	-0.009	0.045	0.048	-0.038	-0.020	-0.045	-0.015	0.015
G16	Plan to check the land registry	0.001	0.033	-0.058	-0.004	-0.071	0.043	0.011	-0.027
G20	Make effort to check land registry	0.012	-0.018	0.017	-0.046	0.029	-0.001	-0.036	0.062
G22	Intend to check land registry	-0.013	-0.014	0.038	0.049	0.039	-0.040	0.025	-0.036
G04	Plan to monitor my accounts and cards	0.003	-0.056	0.048	0.150	0.024	-0.075	0.002	0.021
G11	Make effort to monitor accounts/cards	0.004	0.093	-0.128	-0.413	0.029	0.131	-0.042	-0.003
G13	Intend to monitor my accounts and cards	-0.007	-0.026	0.064	0.211	-0.049	-0.039	0.034	-0.018
G43	Plan to secure my financial documents	0.001	0.007	0.095	0.064	-0.052	-0.025	0.005	-0.022
G47	Make an effort to secure documents	0.011	-0.026	-0.002	0.090	-0.012	0.006	0.042	-0.048
G49	Intend to secure my financial documents	-0.012	0.019	-0.094	-0.156	0.065	0.019	-0.048	0.071
G34	Plan to use secure passwords	-0.024	0.013	-0.013	0.126	0.004	-0.076	-0.034	0.071
G39	Make an effort to use secure passwords	-0.017	-0.032	0.107	0.049	-0.142	0.105	0.079	-0.062
G40	Intend to use secure passwords	0.044	0.020	-0.100	-0.187	0.148	-0.031	-0.047	-0.010
G61	Plan to click on links in e-mails	-0.017	0.029	0.038	-0.057	-0.061	0.000	0.097	-0.067
G65	Make an effort to click on links	0.100	-0.120	-0.033	0.046	0.036	-0.043	-0.089	0.110
G67	Intend to click on links in e-mails	-0.077	0.085	-0.008	0.015	0.028	0.041	-0.015	-0.036
G70	Plan to give personal info over phone	-0.009	-0.006	-0.049	0.091	-0.046	-0.008	-0.033	0.018
G74	Make effort-give personal info over phone	-0.008	0.013	0.071	-0.123	-0.064	0.048	0.073	-0.052
G76	Intend to give personal infor over phone	0.016	-0.005	-0.015	0.019	0.103	-0.035	-0.032	0.029
G52	Plan to use "remember my password"	0.084	-0.004	0.025	-0.150	-0.023	0.050	-0.022	-0.001
G56	Make effort to use "remember password"	-0.080	0.012	-0.020	0.250	0.071	-0.121	0.077	-0.117
G58	Intend to use "remember my password"	-0.013	-0.007	-0.007	-0.075	-0.041	0.059	-0.048	0.107
H01	Monitor credit card accounts	0.000	0.014	-0.049	-0.009	0.108	0.016	-0.042	0.012
H02	Monitor bank account balances	0.000	-0.014	0.049	0.009	-0.108	-0.016	0.042	-0.012
H03	Request a copy of my credit report	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H04	Check land registry office records	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H07	Use a locked mailbox for incoming mail	0.104	-0.015	-0.114	0.020	0.032	-0.036	0.051	0.115
H08	Shred financial or important documents	-0.128	0.231	0.037	-0.173	0.038	-0.076	-0.016	-0.122
H09	Keep financial info in secure place	0.050	-0.209	0.043	0.151	-0.058	0.097	-0.020	0.037
H05	Use hard-to-break passwords	-0.153	0.113	-0.019	-0.202	-0.003	0.044	0.118	-0.097
H06	Have different passwords	0.153	-0.113	0.019	0.202	0.003	-0.044	-0.118	0.097
H12	Click on link in e-mail	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H10	Use "remember my password"	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H11	Give personal information over the phone	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
I01	Worry about identity theft	-0.071	0.092	0.009	-0.043	-0.022	-0.056	0.175	-0.079
I02	Good possibility I will be a victim	0.040	-0.050	0.123	0.070	0.064	-0.048	-0.068	-0.064
I03	Know many people who have been victims	0.063	-0.007	-0.138	-0.110	-0.096	0.158	0.090	-0.025
I04	People like me are likely to be victims	-0.019	-0.031	-0.037	0.047	0.024	-0.010	-0.160	0.159
I06	Identity fraud would severely affect	-0.079	0.028	-0.043	-0.035	0.084	-0.071	0.044	-0.046
I07	Identity fraud is a serious problem	0.040	-0.009	0.033	0.038	-0.033	0.025	0.056	-0.037
I08	Threat is too serious to ignore	-0.004	-0.069	0.044	0.061	-0.019	0.046	-0.104	0.046
I09	Identity fraud is hard to recover from	0.042	0.052	-0.037	-0.066	-0.030	-0.003	0.009	0.034

Intention

		Credit	Land	Monitor	Physical	Password	Click on	Info Over	Remember
		Report	Registry	Accounts	Security	Security	Link	Phone	Password
		Intent	Intent	Intent	Intent	Intent	Intent	Intent	Intent
G24	Check my credit report (good)	-0.373	0.016	0.056	0.036	0.037	0.013	0.121	0.035
G27	Check my credit report (valuable)	0.249	-0.153	-0.091	-0.037	0.012	0.008	-0.102	0.085
G30	Check my credit report (interesting)	0.091	0.149	0.045	0.006	-0.049	-0.022	-0.006	-0.125
G15	Check land registry (good)	-0.061	-0.147	-0.066	-0.102	0.014	0.026	0.010	-0.166
G18	Check land registry (valuable)	-0.030	0.025	0.025	0.022	0.078	-0.043	-0.020	0.084
G21	Check land registry (interesting)	0.093	0.118	0.039	0.077	-0.097	0.021	0.011	0.073
G03	Monitor my accounts and cards (good)	0.004	-0.184	-0.146	0.023	0.115	0.050	-0.131	0.212
G07	Monitor bank account/cards (valuable)	-0.120	0.081	-0.124	-0.007	0.144	-0.098	0.031	-0.135
G10	Monitor bank account/cards (interesting)	0.212	0.188	0.495	-0.030	-0.476	0.089	0.184	-0.140
G42	Secure my financial documents (good)	-0.066	-0.029	-0.106	0.022	0.068	0.022	-0.106	0.196
G45	Secure my financial documents (valuable)	-0.238	0.102	-0.005	0.027	0.022	-0.171	-0.117	-0.058
G48	Secure my financial documents (interesting)	0.353	-0.082	0.134	-0.057	-0.106	0.171	0.262	-0.167
G33	Use secure passwords (good)	-0.201	0.012	-0.035	-0.004	-0.030	0.009	-0.058	-0.065
G36	Use secure passwords (valuable)	0.093	-0.039	-0.023	0.030	0.310	0.021	-0.259	0.054
G38	Use secure passwords (pleasant)	0.135	0.033	0.071	-0.032	-0.343	-0.036	0.389	0.015
G60	Click on a link in an e-mail (good)	0.076	0.002	0.100	0.096	-0.091	0.140	0.101	-0.008
G63	Click on a link in an e-mail (valuable)	0.078	-0.092	-0.109	0.010	-0.031	0.113	-0.088	-0.066
G66	Click on a link in an e-mail (interesting)	-0.178	0.105	0.015	-0.120	0.140	-0.291	-0.011	0.087
G69	Give personal info over phone (good)	0.156	0.153	0.041	-0.029	-0.030	-0.141	0.405	-0.035
G72	Give personal info over phone (valuable)	-0.124	0.116	0.019	0.044	0.008	0.541	-0.217	-0.196
G75	Give personal info over phone (interesting)	-0.047	-0.256	-0.058	-0.010	0.024	-0.335	-0.215	0.208
G51	Use "remember my password" (good)	0.244	0.007	-0.008	0.171	-0.205	0.382	-0.171	0.422
G54	Use "remember my password" (valuable)	-0.173	0.100	0.030	0.054	-0.002	-0.137	0.096	0.081
G57	Use "remember my password" (interesting)	-0.035	-0.109	-0.024	-0.206	0.182	-0.193	0.050	-0.453
G02	Most important people think I should	0.161	-0.024	0.011	-0.049	-0.111	-0.109	0.028	-0.206
G06	Friends protect their personal info	0.599	-0.215	0.135	0.325	-0.168	-0.170	0.064	0.052
G09	Expected that I protect personal info	-0.084	-0.275	-0.040	0.081	0.094	0.263	-0.060	0.092
G12	Most approve protecting personal info	-0.419	0.419	-0.046	-0.210	0.115	-0.054	-0.005	0.095
G23	Check my credit report (easy)	0.526	0.217	0.091	-0.130	0.109	0.044	0.038	-0.067
G26	Checking my credit report is up to me	-0.286	-0.152	-0.211	0.107	-0.357	0.188	-0.148	0.057
G28	If wanted, could check my credit report	-0.193	-0.051	0.102	0.017	0.211	-0.195	0.093	0.007
G14	Check land registry (easy)	0.152	0.364	-0.001	-0.099	-0.109	-0.023	0.054	0.044
G17	Check land registry up to me	-0.300	-0.278	-0.045	0.219	-0.052	0.044	0.093	-0.101
G19	If wanted could check land registry	0.115	-0.087	0.039	-0.095	0.139	-0.016	-0.123	0.045
G01	Monitor my accounts and cards (easy)	0.432	-0.268	0.140	-0.117	-0.039	0.099	0.008	-0.091
G05	If I monitor accounts/cards is up to me	-0.380	0.080	-0.115	0.138	-0.181	0.086	-0.029	0.041
G08	If I wanted to I could monitor accounts	0.013	0.147	-0.004	-0.038	0.213	-0.168	0.022	0.036
G41	Secure my financial documents (easy)	0.147	0.201	0.350	-0.283	0.087	-0.093	0.194	-0.134
G44	Whether I secure documents is up to me	-0.318	-0.002	-0.078	0.101	-0.256	0.102	-0.267	-0.115
G46	If I wanted to, I could secure documents	0.166	-0.176	-0.237	0.157	0.161	-0.013	0.076	0.225
G32	Use secure passwords (easy)	0.089	0.050	0.026	-0.079	0.069	-0.345	0.225	0.156
G35	Whether use secure passwords is up to me	-0.314	0.020	-0.104	-0.002	-0.221	0.178	-0.223	-0.091
G37	If wanted, could use secure passwords	0.187	-0.060	0.065	0.071	0.126	0.151	-0.008	-0.059
G59	Click on a link in an e-mail (easy)	-0.268	0.145	0.044	0.127	0.004	0.085	-0.278	0.098
G62	Click on a link in an e-mail is up to me	-0.035	-0.053	0.377	-0.184	-0.317	0.173	0.260	-0.022
G64	If wanted could click on link in e-mail	0.270	-0.131	-0.123	-0.086	0.062	-0.120	0.219	-0.092
G68	Giving personal info over phone (easy)	-0.090	-0.040	0.074	0.263	-0.150	0.062	-0.133	0.083

G71	Give personal info over phone up to me	-0.131	0.011	-0.273	-0.118	-0.230	0.041	-0.101	0.269
G73	If wanted, give personal info over phone	0.116	0.035	-0.004	-0.218	0.197	-0.069	0.149	-0.142
G50	Use "remember my password" (easy)	0.044	-0.157	0.006	0.072	0.090	-0.081	-0.164	0.029
G53	Whether use "remember password" up to me	-0.017	-0.082	-0.172	-0.270	-0.031	0.075	-0.077	-0.112
G55	If wanted could use "remember password"	-0.028	0.180	0.092	0.091	-0.059	0.026	0.183	0.039
G25	Plan to check my credit report	**0.937**	-0.034	0.073	-0.148	0.010	-0.037	0.030	0.066
G29	Make an effort to check my credit report	**0.956**	-0.013	-0.136	-0.030	0.035	0.001	-0.052	0.027
G31	Intend to check my credit report	**0.911**	0.048	0.067	0.184	-0.047	0.037	0.023	-0.095
G16	Plan to check the land registry	-0.090	**0.923**	0.030	0.024	-0.031	-0.064	-0.010	-0.040
G20	Make effort to check land registry	0.024	**0.959**	-0.012	0.000	0.018	0.048	0.007	-0.056
G22	Intend to check land registry	0.062	**0.962**	-0.017	-0.023	0.012	0.014	0.002	0.095
G04	Plan to monitor my accounts and cards	-0.066	-0.056	**0.924**	0.044	0.160	-0.006	-0.034	-0.102
G11	Make effort to monitor accounts/cards	-0.021	0.222	**0.811**	-0.038	-0.231	-0.041	0.081	0.110
G13	Intend to monitor my accounts and cards	0.083	-0.137	**0.934**	-0.010	0.043	0.041	-0.037	0.006
G43	Plan to secure my financial documents	0.037	-0.055	-0.007	**0.907**	-0.023	-0.022	-0.087	0.010
G47	Make an effort to secure documents	-0.028	0.087	0.068	**0.908**	-0.154	0.032	-0.074	0.023
G49	Intend to secure my financial documents	-0.009	-0.033	-0.062	**0.894**	0.180	-0.010	0.164	-0.033
G34	Plan to use secure passwords	-0.011	0.066	-0.107	0.093	**0.910**	0.095	0.024	-0.123
G39	Make an effort to use secure passwords	-0.072	-0.095	-0.072	0.105	**0.908**	0.046	-0.130	-0.038
G40	Intend to use secure passwords	0.089	0.031	0.192	-0.212	**0.848**	-0.150	0.114	0.173
G61	Plan to click on links in e-mails	-0.185	0.047	0.067	0.083	-0.061	**0.906**	0.133	0.117
G65	Make an effort to click on links	0.128	-0.098	-0.045	0.154	0.070	**0.837**	-0.146	-0.138
G67	Intend to click on links in e-mails	0.069	0.045	-0.026	-0.232	-0.004	**0.876**	0.001	0.012
G70	Plan to give personal info over phone	0.213	0.006	-0.073	0.048	-0.059	-0.060	**0.901**	0.030
G74	Make effort-give personal info over phone	-0.335	-0.065	-0.028	0.041	0.130	0.117	**0.805**	-0.153
G76	Intend to give personal infor over phone	0.086	0.052	0.098	-0.084	-0.057	-0.044	**0.903**	0.107
G52	Plan to use "remember my password"	0.019	-0.114	0.077	-0.086	0.011	-0.021	0.077	**0.916**
G56	Make effort to use "remember password"	0.016	0.036	-0.148	0.158	-0.009	0.319	-0.245	**0.817**
G58	Intend to use "remember my password"	-0.034	0.083	0.056	-0.056	-0.003	-0.268	0.144	**0.899**
H01	Monitor credit card accounts	-0.045	0.114	-0.121	-0.025	0.018	0.052	-0.055	-0.054
H02	Monitor bank account balances	0.045	-0.114	0.121	0.025	-0.018	-0.052	0.055	0.054
H03	Request a copy of my credit report	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H04	Check land registry office records	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H07	Use a locked mailbox for incoming mail	0.066	0.134	-0.106	-0.052	0.178	-0.157	0.210	0.395
H08	Shred financial or important documents	-0.032	-0.208	0.236	-0.385	0.025	0.184	-0.173	-0.121
H09	Keep financial info in secure place	-0.016	0.106	-0.151	0.403	-0.146	-0.066	0.020	-0.158
H05	Use hard-to-break passwords	-0.256	0.054	0.021	-0.128	0.409	-0.082	0.206	0.053
H06	Have different passwords	0.256	-0.054	-0.021	0.128	-0.409	0.082	-0.206	-0.053
H12	Click on link in e-mail	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H10	Use "remember my password"	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
H11	Give personal information over the phone	0.000	0.000	0.000	0.000	0.000	0.000	0.000	0.000
I01	Worry about identity theft	-0.229	0.163	0.021	-0.057	0.260	0.108	0.155	0.097
I02	Good possibility I will be a victim	0.009	-0.106	0.092	0.081	-0.200	0.161	-0.054	0.030
I03	Know many people who have been victims	0.189	0.109	0.040	-0.194	-0.107	-0.315	0.018	-0.071
I04	People like me are likely to be victims	0.073	-0.123	-0.143	0.110	0.037	-0.043	-0.104	-0.072
I06	Identity fraud would severely affect	-0.158	0.013	0.007	-0.020	0.037	0.299	-0.075	-0.097
I07	Identity fraud is a serious problem	0.174	-0.047	-0.087	0.086	-0.079	-0.160	0.003	0.166
I08	Threat is too serious to ignore	0.055	0.012	-0.001	-0.016	0.070	-0.132	0.010	-0.034
I09	Identity fraud is hard to recover from	-0.074	0.021	0.079	-0.050	-0.030	0.001	0.060	-0.034

Behavioural Components (Formative), PMT variables and P values

		Monitor	Monitor	Use	Use	Use			
		Agencies	Accounts	Physical	Password	Risky	Vulnerab-	Severity	P
		Behaviour	Behaviour	Security	Security	Behaviours	ility		Value
G24	Check my credit report (good)	0.031	-0.057	-0.039	0.086	-0.043	-0.007	0.111	<0.001
G27	Check my credit report (valuable)	-0.094	0.027	-0.004	0.103	0.042	-0.041	-0.018	<0.001
G30	Check my credit report (interesting)	0.072	0.025	0.042	-0.194	-0.004	0.050	-0.087	<0.001
G15	Check land registry (good)	0.006	0.028	-0.020	0.083	-0.044	0.029	0.015	<0.001
G18	Check land registry (valuable)	-0.027	-0.024	-0.008	-0.002	0.020	-0.092	0.048	<0.001
G21	Check land registry (interesting)	0.023	-0.001	0.028	-0.079	0.022	0.070	-0.066	<0.001
G03	Monitor my accounts and cards (good)	0.005	-0.046	0.069	0.040	-0.088	0.006	0.044	<0.001
G07	Monitor bank account/cards (valuable)	-0.018	0.027	-0.146	0.097	0.068	-0.084	0.017	<0.001
G10	Monitor bank account/cards (interesting)	0.024	0.034	0.142	-0.252	0.036	0.144	-0.112	<0.001
G42	Secure my financial documents (good)	-0.045	-0.030	-0.132	0.137	-0.003	-0.024	0.061	<0.001
G45	Secure my financial documents (valuable)	-0.043	-0.017	0.043	-0.017	0.095	0.009	-0.018	<0.001
G48	Secure my financial documents (interesting)	0.104	0.055	0.109	-0.143	-0.105	0.018	-0.053	<0.001
G33	Use secure passwords (good)	0.002	0.033	-0.056	0.056	0.007	-0.006	-0.035	<0.001
G36	Use secure passwords (valuable)	-0.054	-0.059	0.000	-0.024	0.085	0.015	0.043	<0.001
G38	Use secure passwords (pleasant)	0.063	0.031	0.069	-0.040	-0.114	-0.012	-0.009	<0.001
G60	Click on a link in an e-mail (good)	-0.088	-0.049	-0.046	0.130	-0.035	-0.017	-0.034	<0.001
G63	Click on a link in an e-mail (valuable)	0.032	0.052	0.050	-0.011	-0.019	0.011	0.007	<0.001
G66	Click on a link in an e-mail (interesting)	0.062	-0.006	-0.007	-0.134	0.061	0.006	0.030	<0.001
G69	Give personal info over phone (good)	-0.113	-0.005	0.051	-0.026	0.052	-0.080	-0.021	<0.001
G72	Give personal info over phone (valuable)	0.074	0.017	-0.010	-0.044	-0.006	0.066	0.000	<0.001
G75	Give personal info over phone (interesting)	0.049	-0.010	-0.042	0.065	-0.047	0.022	0.021	<0.001
G51	Use "remember my password" (good)	-0.072	-0.061	-0.102	0.044	-0.037	-0.013	-0.028	<0.001
G54	Use "remember my password" (valuable)	0.052	0.023	-0.015	-0.026	0.054	-0.007	0.062	<0.001
G57	Use "remember my password" (interesting)	0.009	0.030	0.105	-0.011	-0.024	0.019	-0.040	<0.001
G02	Most important people think I should	-0.062	0.032	-0.009	0.173	0.090	-0.003	-0.026	<0.001
G06	Friends protect their personal info	-0.015	-0.045	0.110	-0.073	0.105	-0.038	-0.157	<0.001
G09	Expected that I protect personal info	0.080	-0.067	-0.019	-0.038	-0.070	0.042	0.045	<0.001
G12	Most approve protecting personal info	-0.007	0.058	-0.033	-0.103	-0.083	-0.018	0.070	<0.001
G23	Check my credit report (easy)	-0.047	0.042	0.054	-0.033	-0.049	-0.011	-0.060	<0.001
G26	Checking my credit report is up to me	0.051	0.147	-0.072	0.070	0.015	0.071	0.030	<0.001
G28	If wanted, could check my credit report	-0.004	-0.158	0.016	-0.032	0.028	-0.051	0.024	<0.001
G14	Check land registry (easy)	0.080	-0.035	0.075	0.012	-0.032	-0.024	-0.090	<0.001
G17	Check land registry up to me	-0.075	-0.073	-0.098	0.078	0.050	0.031	0.045	<0.001
G19	If wanted could check land registry	-0.008	0.091	0.016	-0.075	-0.013	-0.005	0.042	<0.001
G01	Monitor my accounts and cards (easy)	0.033	0.192	-0.003	-0.089	-0.172	0.049	-0.059	<0.001
G05	If I monitor accounts/cards is up to me	-0.058	-0.155	-0.030	0.141	0.110	0.082	0.012	<0.001
G08	If I wanted to I could monitor accounts	0.029	-0.007	0.032	-0.065	0.036	-0.123	0.037	<0.001
G41	Secure my financial documents (easy)	-0.165	-0.029	0.031	-0.043	-0.044	-0.038	0.046	<0.001
G44	Whether I secure documents is up to me	0.099	-0.083	0.019	0.019	0.095	0.074	0.052	<0.001
G46	If I wanted to, I could secure documents	0.054	0.103	-0.045	0.021	-0.050	-0.035	-0.089	<0.001
G32	Use secure passwords (easy)	-0.064	0.121	-0.046	0.122	-0.078	-0.029	-0.048	<0.001
G35	Whether use secure passwords is up to me	0.059	0.009	0.085	-0.069	0.134	0.081	0.039	<0.001
G37	If wanted, could use secure passwords	0.006	-0.112	-0.031	-0.048	-0.045	-0.043	0.009	<0.001
G59	Click on a link in an e-mail (easy)	-0.014	0.045	-0.167	0.108	0.048	-0.068	0.027	<0.001
G62	Click on a link in an e-mail is up to me	-0.071	-0.016	-0.094	0.224	-0.033	0.189	-0.002	0.217
G64	If wanted could click on link in e-mail	0.029	-0.041	0.184	-0.153	-0.040	0.028	-0.026	<0.001
G68	Giving personal info over phone (easy)	-0.105	0.029	-0.108	0.192	0.053	-0.025	-0.057	<0.001

G71	Give personal info over phone up to me	-0.016	0.014	-0.062	0.245	0.029	0.091	0.055	0.278
G73	If wanted, give personal info over phone	0.102	-0.030	0.116	-0.239	-0.056	0.002	0.040	<0.001
G50	Use "remember my password" (easy)	-0.059	0.032	-0.150	0.205	0.009	-0.100	0.012	<0.001
G53	Whether use "remember password" up to me	0.124	0.019	0.080	-0.093	-0.001	0.099	0.023	0.046
G55	If wanted could use "remember password"	-0.019	-0.038	0.083	-0.122	-0.007	0.029	-0.024	<0.001
G25	Plan to check my credit report	0.049	-0.008	0.019	0.068	-0.011	-0.009	0.012	<0.001
G29	Make an effort to check my credit report	-0.034	0.036	0.011	-0.047	-0.011	0.028	-0.013	<0.001
G31	Intend to check my credit report	-0.014	-0.029	-0.031	-0.021	0.024	-0.020	0.001	<0.001
G16	Plan to check the land registry	0.093	-0.038	-0.003	-0.013	0.001	0.026	-0.045	<0.001
G20	Make effort to check land registry	-0.049	0.030	-0.010	-0.003	0.022	-0.019	0.036	<0.001
G22	Intend to check land registry	-0.040	0.007	0.013	0.015	-0.023	-0.006	0.007	<0.001
G04	Plan to monitor my accounts and cards	0.059	-0.080	-0.030	-0.067	0.048	0.043	-0.073	<0.001
G11	Make effort to monitor accounts/cards	-0.141	0.145	0.041	0.107	-0.091	-0.039	0.112	<0.001
G13	Intend to monitor my accounts and cards	0.064	-0.046	-0.006	-0.026	0.031	-0.008	-0.026	<0.001
G43	Plan to secure my financial documents	-0.019	-0.047	0.011	0.065	0.017	0.010	0.008	<0.001
G47	Make an effort to secure documents	0.023	-0.024	-0.049	-0.034	0.044	-0.072	0.028	<0.001
G49	Intend to secure my financial documents	-0.004	0.072	0.039	-0.031	-0.062	0.062	-0.037	<0.001
G34	Plan to use secure passwords	-0.019	-0.008	-0.080	0.006	-0.022	-0.115	0.017	<0.001
G39	Make an effort to use secure passwords	0.019	0.016	0.036	-0.032	0.039	-0.028	-0.006	<0.001
G40	Intend to use secure passwords	0.000	-0.009	0.046	0.028	-0.019	0.154	-0.012	<0.001
G61	Plan to click on links in e-mails	-0.001	0.000	0.000	0.016	-0.009	-0.032	0.001	<0.001
G65	Make an effort to click on links	0.079	-0.048	0.010	-0.051	0.006	-0.007	-0.023	<0.001
G67	Intend to click on links in e-mails	-0.075	0.046	-0.010	0.032	0.004	0.039	0.021	<0.001
G70	Plan to give personal info over phone	-0.058	0.023	-0.040	0.046	0.053	-0.043	0.080	<0.001
G74	Make effort-give personal info over phone	0.151	-0.037	0.033	-0.029	-0.068	0.065	-0.122	<0.001
G76	Intend to give personal infor over phone	-0.077	0.010	0.011	-0.020	0.007	-0.015	0.029	<0.001
G52	Plan to use "remember my password"	0.027	0.068	-0.012	-0.007	-0.054	-0.015	0.044	<0.001
G56	Make effort to use "remember password"	0.022	-0.130	-0.074	0.023	0.121	0.129	-0.101	<0.001
G58	Intend to use "remember my password"	-0.048	0.049	0.079	-0.013	-0.055	-0.102	0.046	<0.001
H01	Monitor credit card accounts	**0.853**	0.023	-0.049	0.025	-0.006	-0.031	0.031	<0.001
H02	Monitor bank account balances	**0.853**	-0.023	0.049	-0.025	0.006	0.031	-0.031	<0.001
H03	Request a copy of my credit report	0.023	**0.921**	-0.005	-0.041	0.099	0.021	0.052	<0.001
H04	Check land registry office records	-0.023	**0.921**	0.005	0.041	-0.099	-0.021	-0.052	<0.001
H07	Use a locked mailbox for incoming mail	-0.085	0.182	**0.562**	-0.279	0.085	0.074	-0.118	<0.001
H08	Shred financial or important documents	-0.039	-0.101	**0.774**	0.143	-0.091	-0.096	0.090	<0.001
H09	Keep financial info in secure place	0.095	-0.030	**0.813**	0.057	0.028	0.040	-0.004	<0.001
H05	Use hard-to-break passwords	0.079	-0.043	-0.004	**0.856**	-0.053	0.021	0.048	<0.001
H06	Have different passwords	-0.079	0.043	0.004	**0.856**	0.053	-0.021	-0.048	<0.001
H12	Click on link in e-mail	-0.065	0.113	0.157	-0.081	**0.544**	0.023	-0.023	<0.001
H10	Use "remember my password"	0.027	-0.098	-0.154	0.079	**0.745**	0.062	-0.009	<0.001
H11	Give personal information over the phone	0.020	0.015	0.039	-0.020	**0.754**	-0.078	0.025	<0.001
I01	Worry about identity theft	-0.040	-0.040	-0.016	0.010	-0.199	**0.779**	0.189	<0.001
I02	Good possibility I will be a victim	-0.045	-0.088	0.055	0.118	-0.021	**0.849**	0.071	<0.001
I03	Know many people who have been victims	0.106	0.121	-0.045	-0.058	0.051	**0.588**	-0.384	<0.001
I04	People like me are likely to be victims	0.009	0.042	-0.010	-0.090	0.174	**0.819**	0.023	<0.001
I06	Identity fraud would severely affect	0.015	0.039	-0.019	0.041	0.011	-0.157	**0.822**	<0.001
I07	Identity fraud is a serious problem	-0.113	-0.030	0.022	-0.020	0.041	0.041	**0.829**	<0.001
I08	Threat is too serious to ignore	0.006	-0.020	0.028	0.020	-0.005	0.203	**0.867**	<0.001
I09	Identity fraud is hard to recover from	0.091	0.012	-0.031	-0.041	-0.045	-0.096	**0.842**	<0.001

Appendix H – Latent Variable Coefficients

	Composite reliability coefficients	Cronbach's alpha coefficients	Average variances extracted	Full co linearity VIFs
Attitudes				
Credit Report	0.875	0.786	0.701	3.690
Land Registry	0.904	0.839	0.758	3.784
Monitor Accounts	0.903	0.785	0.823	1.964
Physical Security	0.789	0.599	0.557	2.936
Secure Passwords	0.804	0.634	0.580	2.119
Click on Link	0.900	0.832	0.751	3.804
Give Personal Info Over Phone	0.832	0.697	0.624	2.720
Remember Password	0.834	0.700	0.627	3.066
Subjective Norm				
	0.857	0.749	0.666	2.009
Perceived Behavioural Control				
Credit Report	0.773	0.559	0.534	2.366
Land Registry	0.835	0.702	0.630	2.046
Monitor Accounts	0.827	0.685	0.616	3.242
Physical Security	0.728	0.438	0.472	2.139
Secure Passwords	0.759	0.524	0.514	2.585
Click on Link	0.805	0.514	0.673	2.738
Give Personal Info Over Phone	0.794	0.483	0.659	2.308
Remember Password	0.698	0.362	0.447	2.121
Intent				
Credit Report	0.954	0.928	0.874	4.251
Land Registry	0.964	0.944	0.900	3.766
Monitor Accounts	0.921	0.869	0.795	2.907
Physical Security	0.930	0.887	0.815	3.672
Secure Passwords	0.919	0.867	0.790	3.947
Click on Link	0.906	0.844	0.763	3.629
Give Personal Info Over Phone	0.904	0.839	0.758	3.143
Remember Password	0.910	0.850	0.771	3.290
Behaviours (Formative)				
Monitor Agencies	0.843	0.626	0.728	1.765
Monitor Accounts	0.917	0.820	0.848	1.601
Use Physical Security	0.764	0.538	0.525	1.723
Use Secure Passwords	0.846	0.635	0.733	1.971
Risky Behaviours	0.725	0.435	0.473	1.672
PMT Variables				
Vulnerability	0.877	0.789	0.704	1.921
Severity	0.906	0.861	0.706	1.862

Appendix I – Item Variable Descriptive Statistics

Var-iable	Label	N	Mean	Std Dev	Skew ness	Kurt osis
G01	Monitor my accounts and cards (easy)	356	6.399	1.095	-2.137	4.617
G02	Most important people think I should	356	6.258	1.245	-1.954	3.657
G03	Monitor my accounts and cards (good)	356	6.612	0.959	-3.262	12.184
G04	Plan to monitor my accounts and cards	356	6.466	1.062	-2.137	3.899
G05	If I monitor accounts/cards is up to me	356	6.559	0.961	-2.583	7.024
G06	Friends protect their personal info	356	4.978	1.408	-0.222	-0.193
G07	Monitor bank account/cards (valuable)	356	6.598	0.912	-3.057	11.310
G08	If I wanted to I could monitor accounts	356	6.618	0.938	-3.068	10.691
G09	Expected that I protect personal info	356	6.430	0.992	-2.077	4.747
G10	Monitor bank account/cards (interesting)	356	5.756	1.323	-0.768	-0.372
G11	Make effort to monitor accounts/cards	356	6.607	0.918	-2.770	8.107
G12	Most approve protecting personal info	356	6.267	1.260	-2.264	5.526
G13	Intend to monitor my accounts and cards	356	6.553	0.919	-2.324	5.397
G14	Check land registry (easy)	222	4.014	1.877	0.013	-0.891
G15	Check land registry (good)	222	4.761	1.606	-0.273	-0.264
G16	Plan to check the land registry	222	3.419	2.047	0.392	-1.104
G17	Check land registry up to me	222	6.095	1.447	-1.720	2.459
G18	Check land registry (valuable)	222	4.423	1.788	-0.205	-0.722
G19	If wanted could check land registry	222	5.477	1.758	-1.071	0.239
G20	Make effort to check land registry	222	3.977	1.920	0.040	-1.095
G21	Check land registry (interesting)	222	3.734	1.824	0.115	-0.747
G22	Intend to check land registry	222	3.815	1.890	0.090	-1.060
G23	Check my credit report (easy)	356	4.851	1.714	-0.223	-0.981
G24	Check my credit report (good)	356	5.211	1.681	-0.661	-0.307
G25	Plan to check my credit report	356	4.157	2.082	-0.024	-1.305
G26	Checking my credit report is up to me	356	6.298	1.141	-1.906	3.979
G27	Check my credit report (valuable)	356	5.163	1.699	-0.659	-0.357
G28	If wanted, could check my credit report	356	6.048	1.364	-1.447	1.447
G29	Make an effort to check my credit report	356	4.511	2.037	-0.248	-1.223
G30	Check my credit report (interesting)	356	4.292	1.860	-0.096	-0.897
G31	Intend to check my credit report	356	4.601	1.974	-0.314	-1.065
G32	Use secure passwords (easy)	356	5.719	1.480	-1.111	0.434
G33	Use secure passwords (good)	356	6.323	1.167	-2.083	4.374
G34	Plan to use secure passwords	356	6.239	1.127	-1.550	2.063
G35	Whether use secure passwords is up to me	356	6.295	1.240	-2.054	4.126
G36	Use secure passwords (valuable)	356	6.278	1.228	-2.112	4.758
G37	If wanted, could use secure passwords	356	6.435	1.012	-2.119	4.840
G38	Use secure passwords (pleasant)	356	5.287	1.631	-0.782	-0.071
G39	Make an effort to use secure passwords	356	6.281	1.080	-1.442	1.130
G40	Intend to use secure passwords	356	6.272	1.052	-1.542	2.054
G41	Secure my financial documents (easy)	356	4.992	1.579	-0.621	-0.214
G42	Secure my financial documents (good)	356	6.368	1.011	-1.956	4.336

Var-iable	Label	N	Mean	Std Dev	Skew ness	Kurt osis
G43	Plan to secure my financial documents	356	5.843	1.373	-1.093	0.456
G44	Whether I secure documents is up to me	356	6.419	1.038	-2.044	4.264
G45	Secure my financial documents (valuable)	356	6.126	1.280	-1.804	3.378
G46	If I wanted to, I could secure documents	356	5.963	1.211	-1.117	0.693
G47	Make an effort to secure documents	356	5.969	1.277	-1.232	0.890
G48	Secure my financial documents (interest)	356	4.899	1.503	-0.282	-0.477
G49	Intend to secure my financial documents	356	5.969	1.204	-1.050	0.311
G50	Use "remember my password" (easy)	356	4.528	2.258	-0.436	-1.281
G51	Use "remember my password" (good)	356	2.963	1.969	0.634	-0.820
G52	Plan to use "remember my password"	356	2.899	2.087	0.726	-0.863
G53	Whether use "remember password" up to me	356	6.258	1.341	-2.032	3.810
G54	Use "remember my password" (valuable)	356	3.671	2.235	0.140	-1.413
G55	If wanted could use "remember password"	356	4.660	2.274	-0.491	-1.235
G56	Make effort to use "remember password"	356	3.034	2.123	0.631	-0.979
G57	Use "remember my password" (interesting)	356	3.551	1.752	0.005	-0.725
G58	Intend to use "remember my password"	356	2.792	2.147	0.780	-0.898
G59	Click on a link in an e-mail (easy)	356	4.065	2.196	-0.044	-1.341
G60	Click on a link in an e-mail (good)	356	2.652	1.573	0.580	-0.514
G61	Plan to click on links in e-mails	356	2.385	1.626	1.064	0.240
G62	Click on a link in an e-mail is up to me	356	6.388	1.250	-2.577	6.976
G63	Click on a link in an e-mail (valuable)	356	2.851	1.678	0.525	-0.533
G64	If wanted could click on link in e-mail	356	4.933	2.136	-0.630	-0.962
G65	Make an effort to click on links	356	2.433	1.674	1.052	0.245
G66	Click on a link in an e-mail (interest)	356	3.295	1.638	0.095	-0.660
G67	Intend to click on links in e-mails	356	2.674	1.765	0.729	-0.508
G68	Giving personal info over phone (easy)	356	3.079	2.026	0.546	-0.956
G69	Give personal info over phone (good)	356	1.860	1.331	1.643	1.956
G70	Plan to give personal info over phone	356	1.812	1.393	1.932	3.180
G71	Give personal info over phone up to me	356	6.466	1.204	-2.769	7.890
G72	Give personal info over phone (valuable)	356	2.607	1.905	1.007	-0.089
G73	If wanted, give personal info over phone	356	4.466	2.325	-0.305	-1.426
G74	Make effort-give personal info over phone	356	1.907	1.540	1.892	2.788
G75	Give personal info over phone (interest)	356	2.421	1.500	0.676	-0.562
G76	Intend to give personal infor over phone	356	1.761	1.305	1.994	3.601
H01	Monitor credit card accounts	356	6.452	1.093	-2.480	6.345
H02	Monitor bank account balances	356	6.654	0.785	-2.651	7.252
H03	Request a copy of my credit report	356	2.798	2.165	0.950	-0.619
H04	Check land registry office records	356	1.767	1.545	2.164	3.741
H05	Use hard-to-break passwords	356	5.593	1.480	-0.921	-0.038
H06	Have different passwords	356	4.992	1.684	-0.581	-0.683
H07	Use a locked mailbox for incoming mail	356	4.427	2.645	-0.304	-1.727
H08	Shred financial or important documents	356	5.744	1.787	-1.341	0.527
H09	Keep financial info in secure place	356	4.514	2.191	-0.318	-1.359

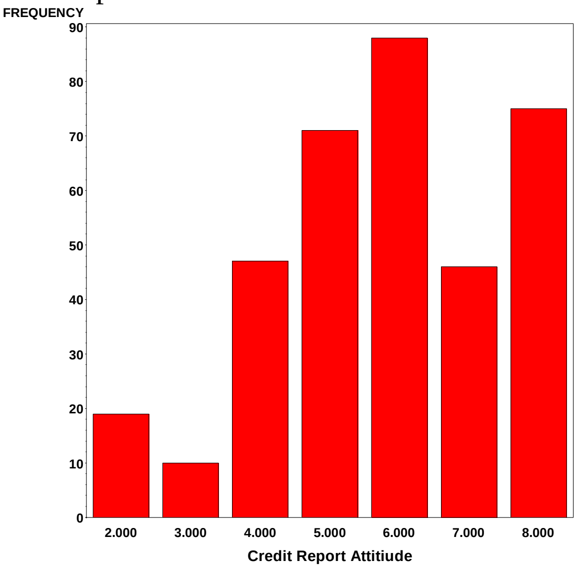
Var- iable	Label	N	Mean	Std Dev	Skew ness	Kurt osis
H10	Use "remember my password"	356	3.056	2.047	0.531	-1.110
H11	Give personal information over the phone	356	1.677	1.177	2.150	4.736
H12	Click on link in e-mail	356	2.402	1.519	1.136	0.541
I01	I worry about identity theft	356	5.376	1.493	-0.974	0.502
I02	Is good possibility I will be a victim	356	5.301	1.360	-0.699	0.195
I03	I know many people who have been victims	356	3.567	1.792	0.167	-1.094
I04	People like me are likely to be victims	356	4.919	1.399	-0.425	-0.290
I05	Worry less about card than other fraud	356	3.649	1.614	-0.007	-0.697
I06	Identity fraud would severely affect	356	5.677	1.260	-0.816	0.249
I07	Identity fraud is a serious problem	356	6.081	1.132	-1.381	2.084
I08	Threat is too serious to ignore	356	5.798	1.251	-0.984	0.489
I09	Identity fraud is hard to recover from	356	5.590	1.324	-0.796	0.182
I10	Card fraud less serious than other fraud	356	3.528	1.750	0.100	-0.951

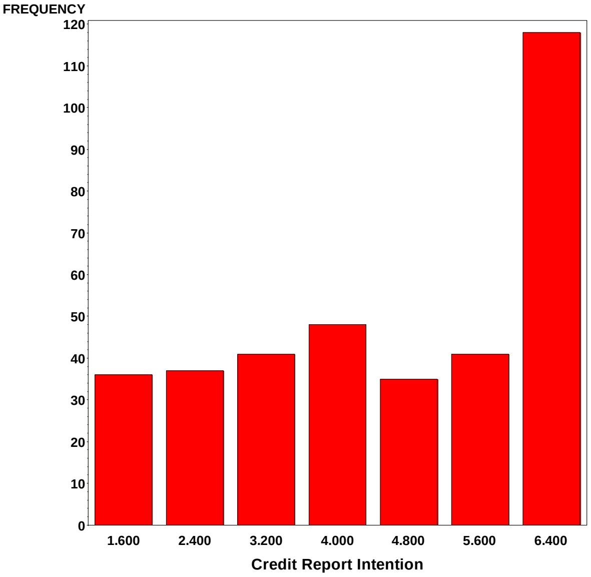
Appendix J – Latent Variable Descriptive Statistics

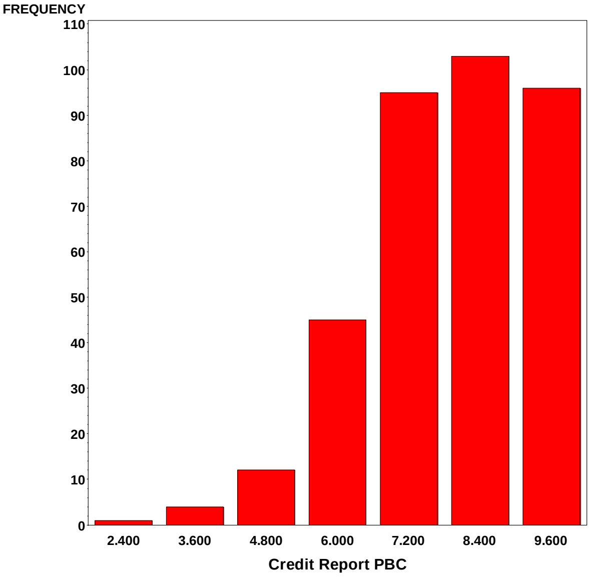
Variable	Label	N	Mean	Std Dev	Skew-ness	Kurt-osis
CRBEL	Credit Report Attitude	356	5.831	1.745	-0.297	-0.476
LRBEL	Check Registry Attitude	222	4.940	1.742	-0.023	-0.428
MABEL	Monitor Accounts Attitude	356	7.279	0.935	-2.448	5.565
PSBEL	Physical Security Attitude	356	7.817	1.244	-0.852	0.638
PWBEL	Secure Password Attitude	356	7.853	1.311	-1.196	1.709
RBCBEL	Click on Link Attitude	356	3.360	1.632	0.419	-0.350
RBPBEL	Info Over Phone Attitude	356	2.883	1.558	0.842	0.088
RBRBEL	Remember Password Attitude	356	4.305	1.996	0.084	-0.777
SUBJNOR	Subjective Norm	356	7.738	1.173	-1.636	2.382
CRCTL	Credit Report PBC	356	7.846	1.406	-0.759	0.716
LRCTL	Check Registry PBC	222	6.522	1.713	-0.832	0.551
MACTL	Monitor Accounts PBC	356	8.302	0.988	-1.879	2.919
PSCTL	Physical Security PBC	356	8.451	1.275	-0.531	-0.264
PWCTL	Secure Password PBC	356	8.571	1.228	-1.052	0.672
RBCCTL	Click on Link PBC	356	5.479	2.165	-0.440	-0.503
RBPCTL	Info Over Phone PBC	356	4.648	2.179	-0.043	-0.831
RBRCTL	Remember Password PBC	356	7.283	2.142	-0.457	-0.575
CRINT	Credit Report Intention	356	4.727	2.031	-0.169	-1.141
LRINT	Check Registry Intention	222	3.947	1.952	0.217	-1.015
MAINT	Monitor Accounts Intention	356	7.318	0.970	-2.216	4.692
PSINT	Physical Security Intention	356	6.561	1.285	-0.890	-0.113
PWINT	Secure Password Intention	356	7.047	1.088	-1.265	0.677
RBCINT	Click on Link Intention	356	2.859	1.688	0.882	0.142
RBPINT	Info Over Phone Intention	356	2.092	1.404	1.694	2.385
RBRINT	Remember Password Intention	356	3.305	2.119	0.622	-0.771
AGENCY	Monitor Agencies	356	2.675	1.864	1.246	0.718
MONIACC	Monitor Card and Bank Accounts	356	7.117	0.941	-2.282	4.823
PHYSSEC	Use Physical Security	356	6.730	2.141	-0.477	-0.539
SECURPW	Use Password Security	356	6.181	1.583	-0.622	-0.403
RISKY	Risky Behaviours	356	3.326	1.516	0.905	0.785
VULNER	PMT Vulnerability	356	6.192	1.415	-0.441	-0.271
SEVERTY	PMT Severity	356	6.880	1.242	-0.684	-0.260

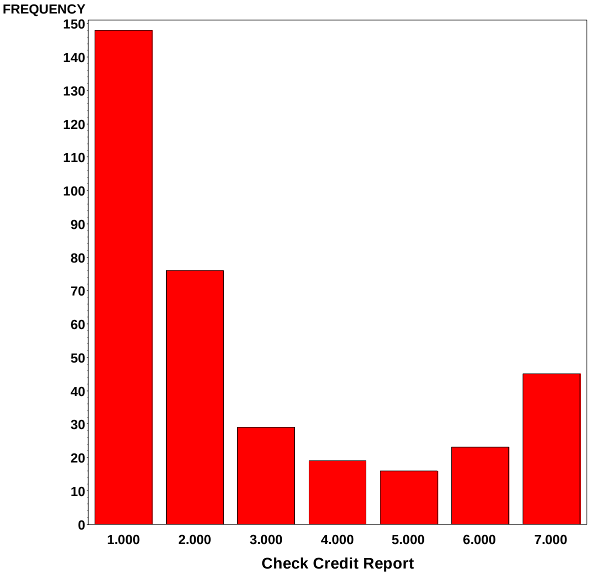
Appendix K – Latent Variable Distributions

Credit Report

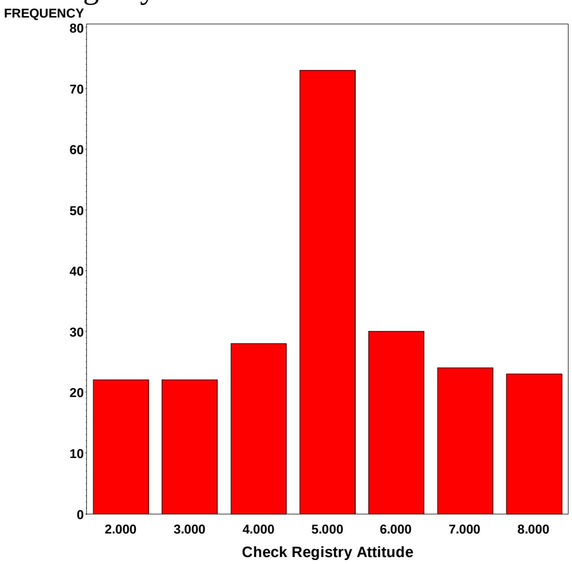


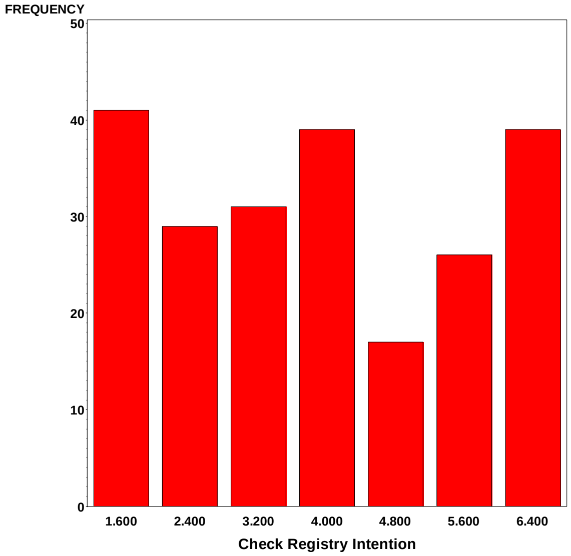


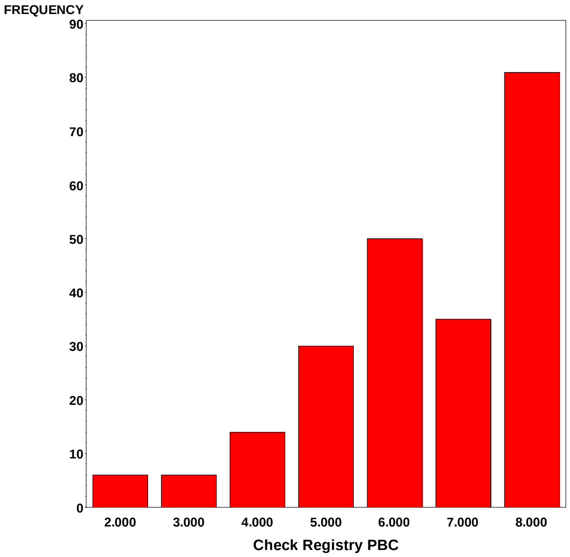


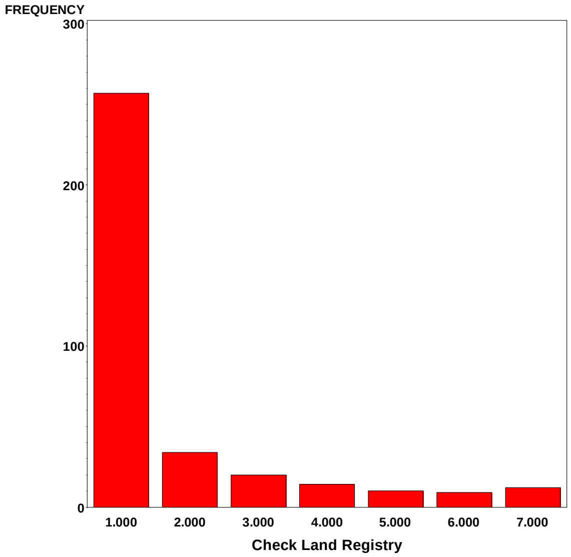


Land Registry

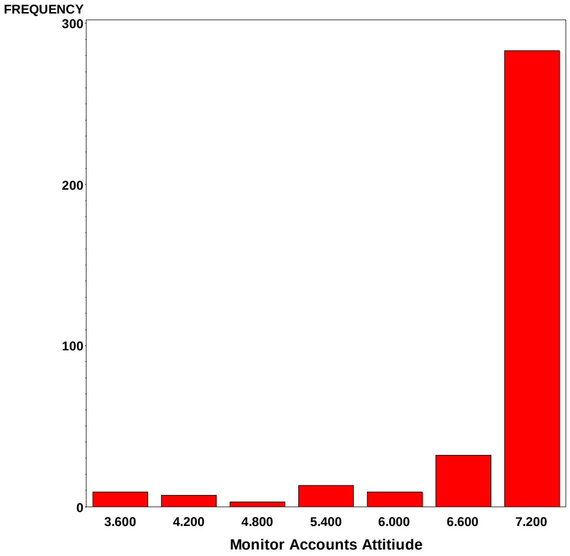


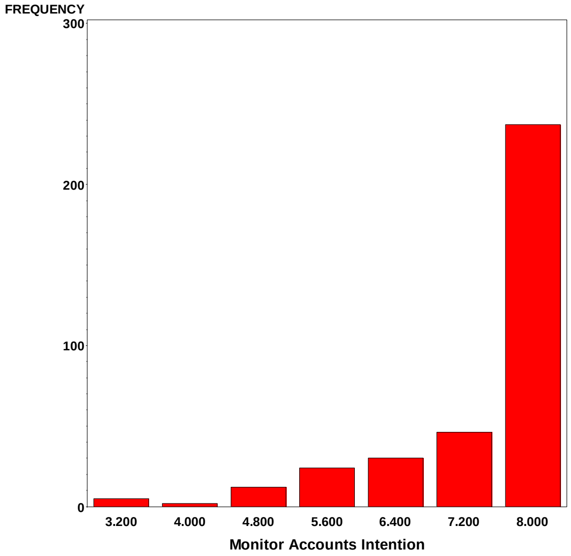


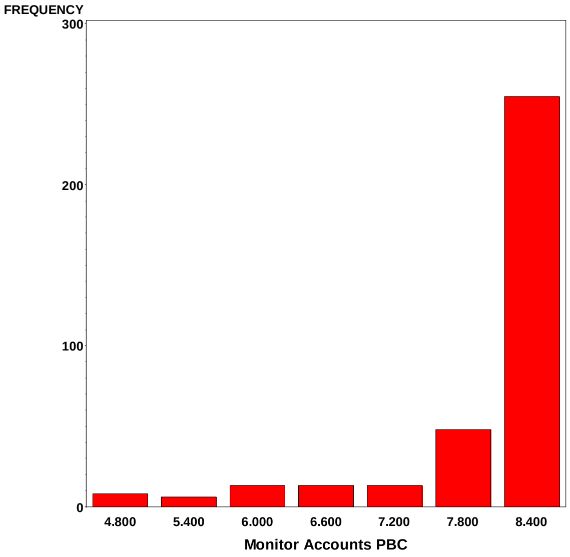


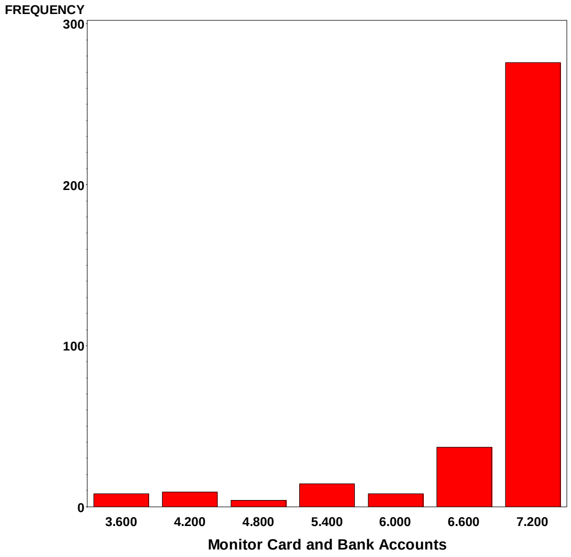


Monitor Accounts

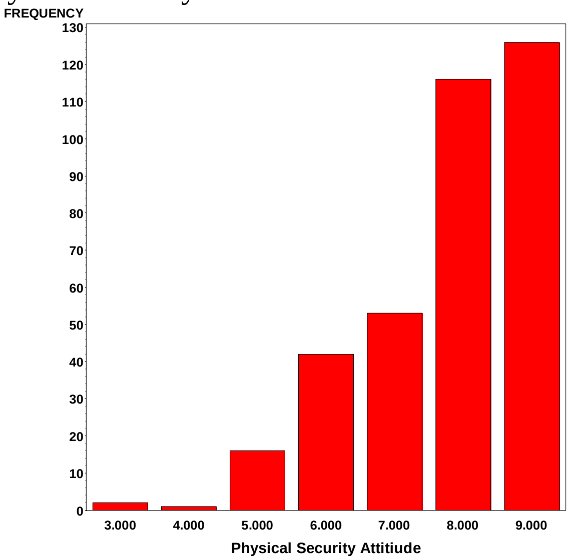


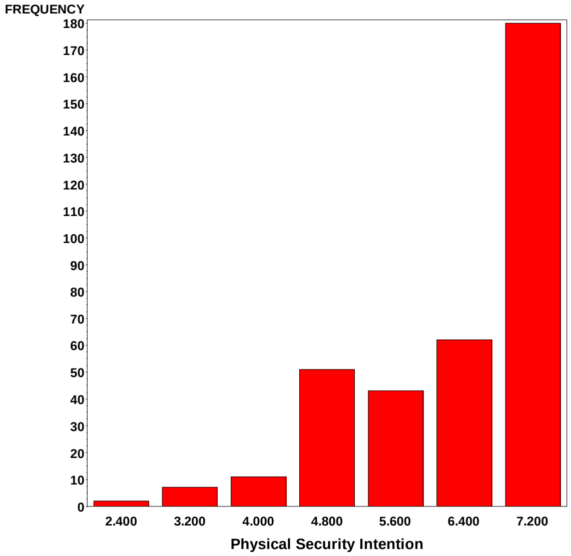


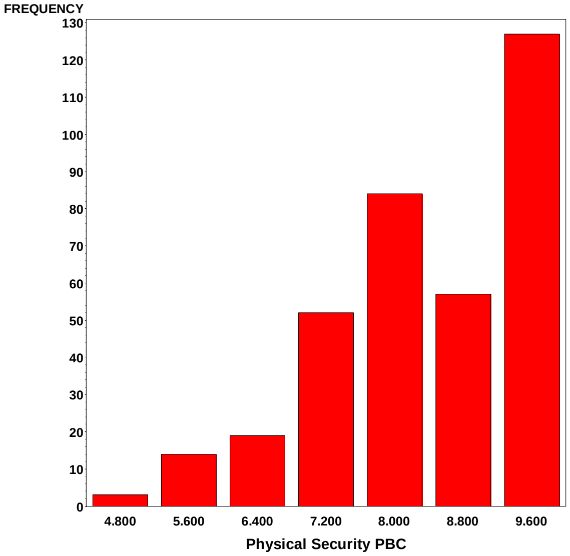


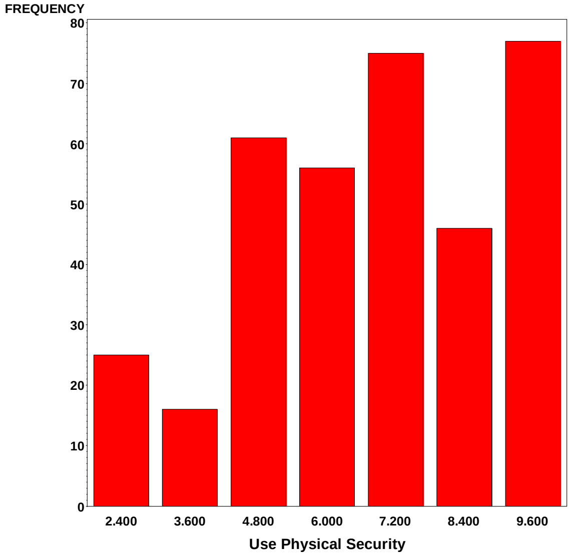


Physical Security

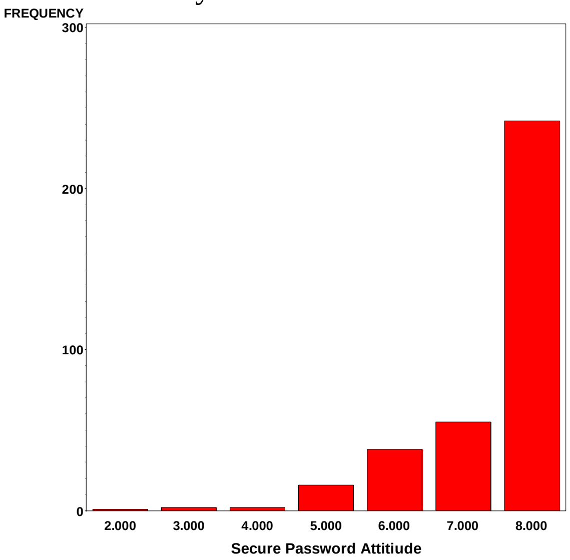


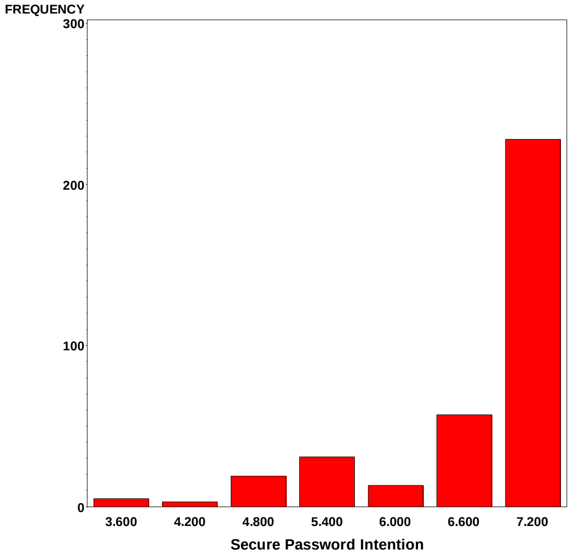


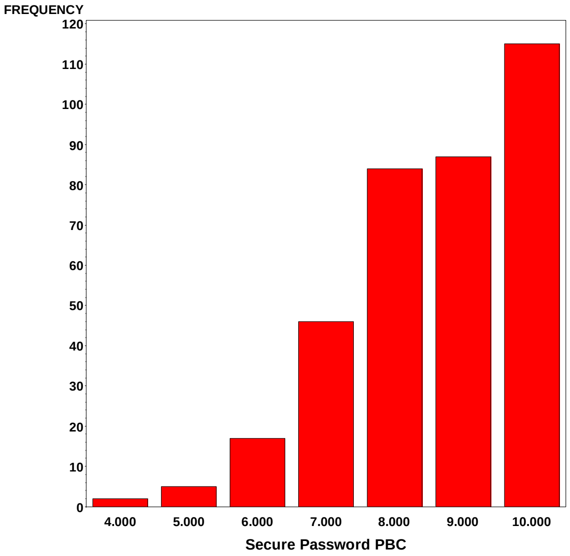


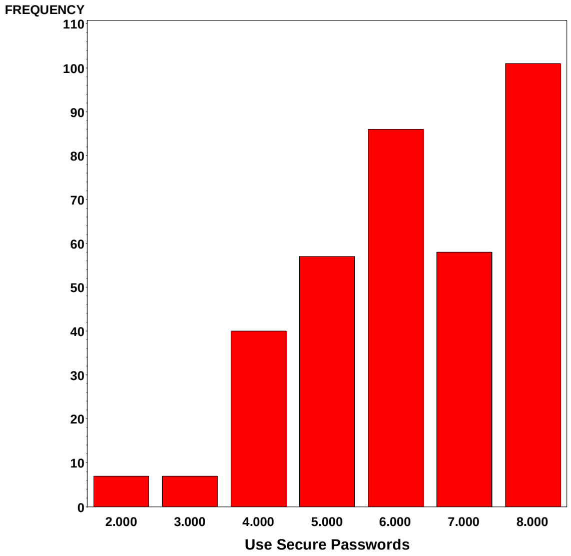


Password Security

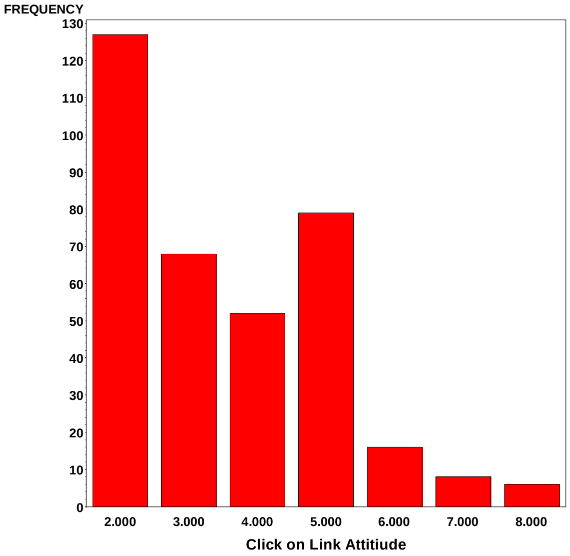


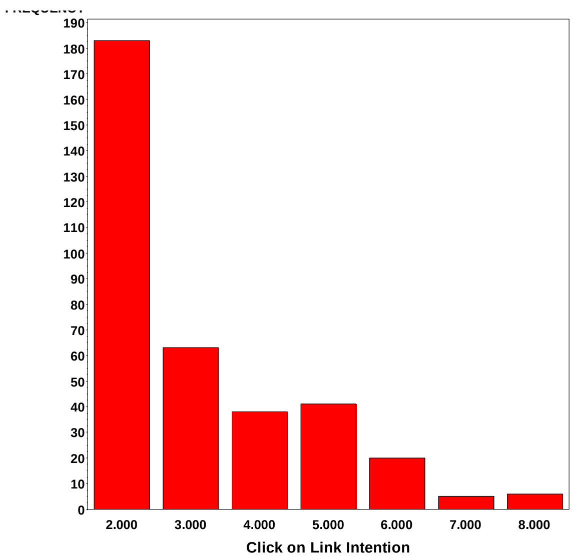


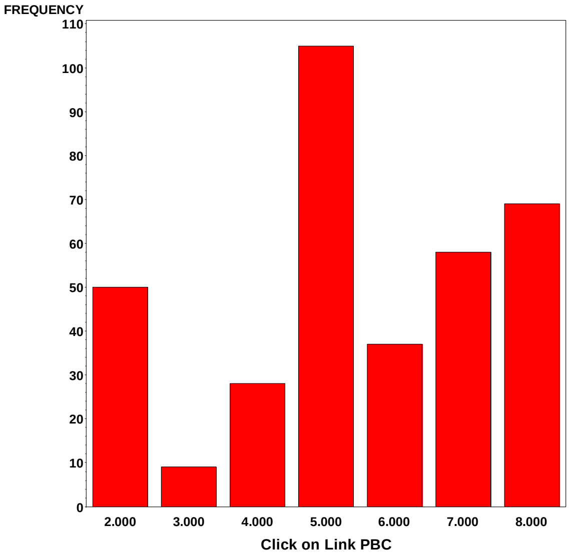


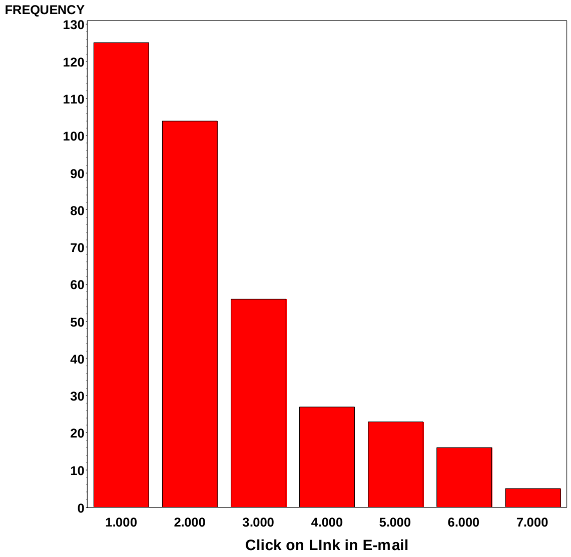


Click on a Link in an E-mail

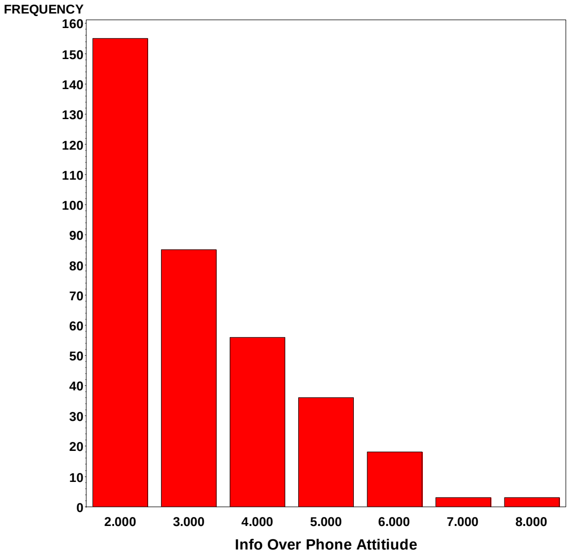


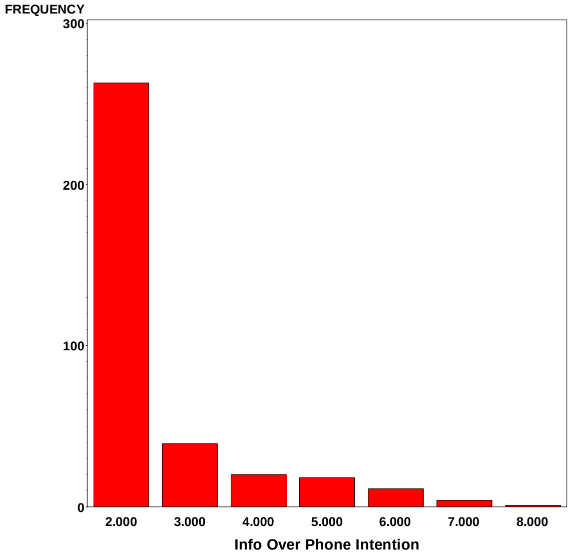


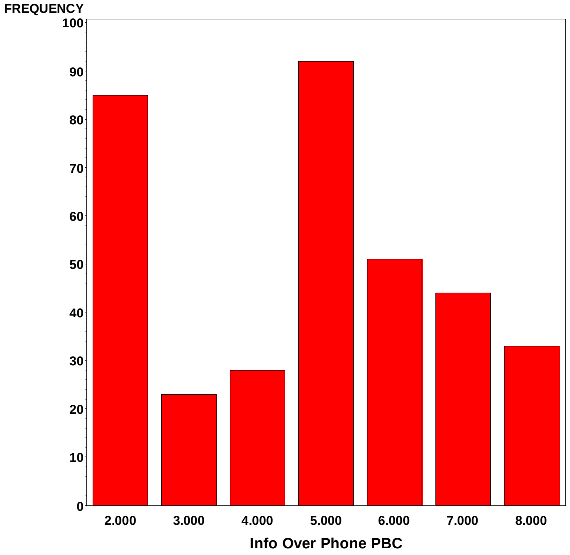


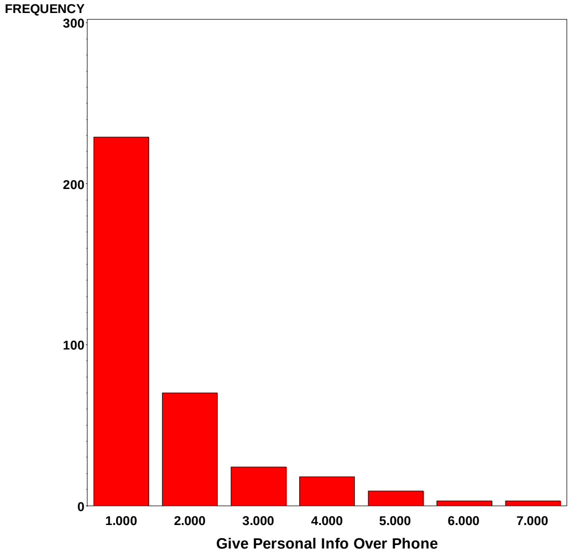


Give Personal Information Over the Phone

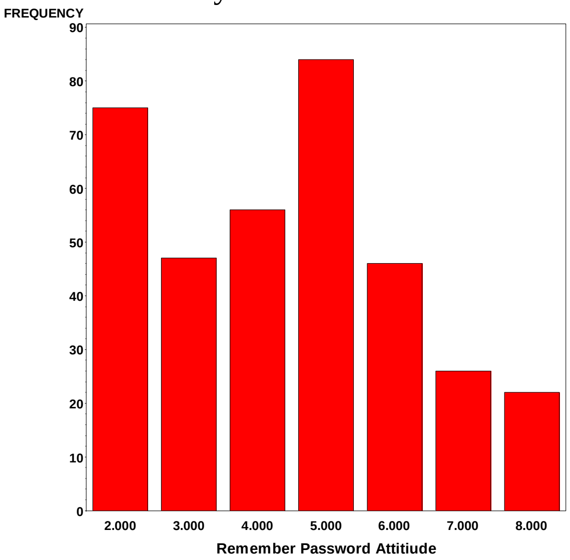


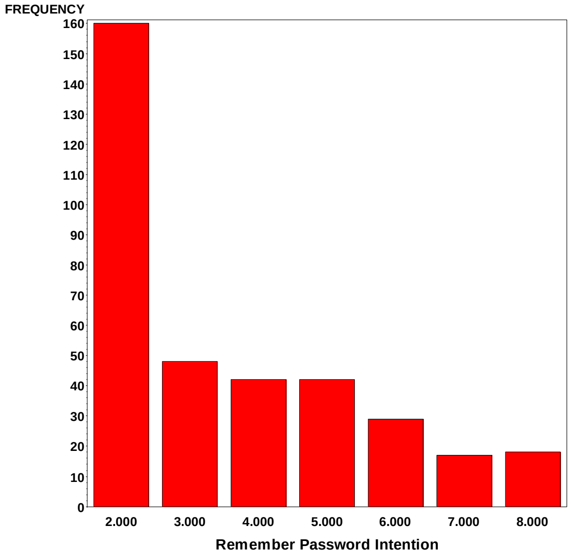


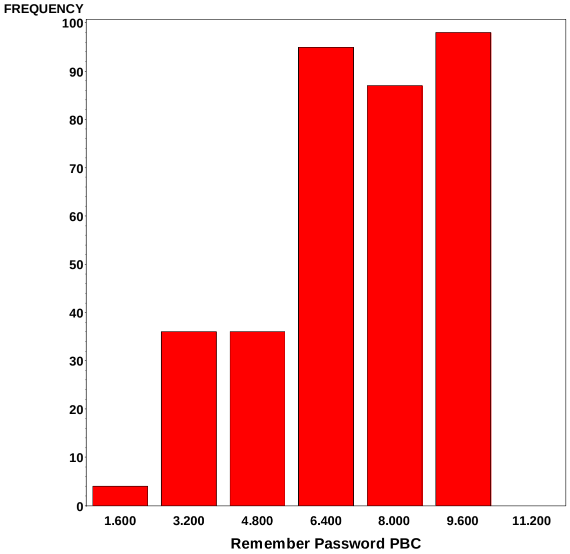


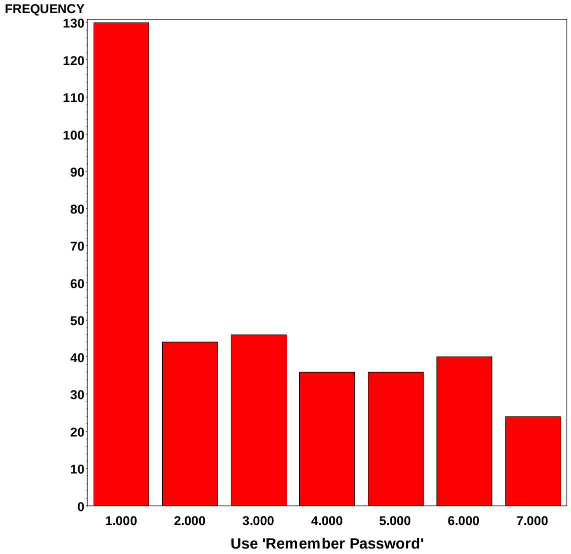


Use 'Remember My Password'

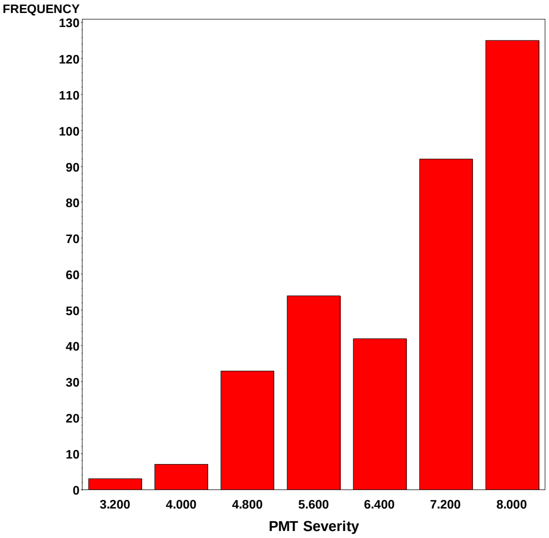


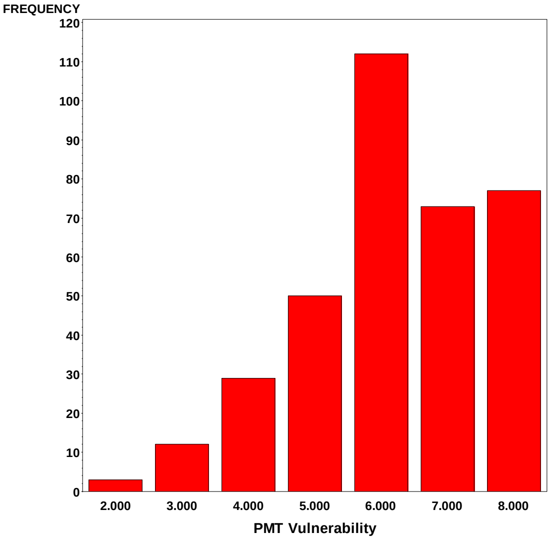






PMT Variables





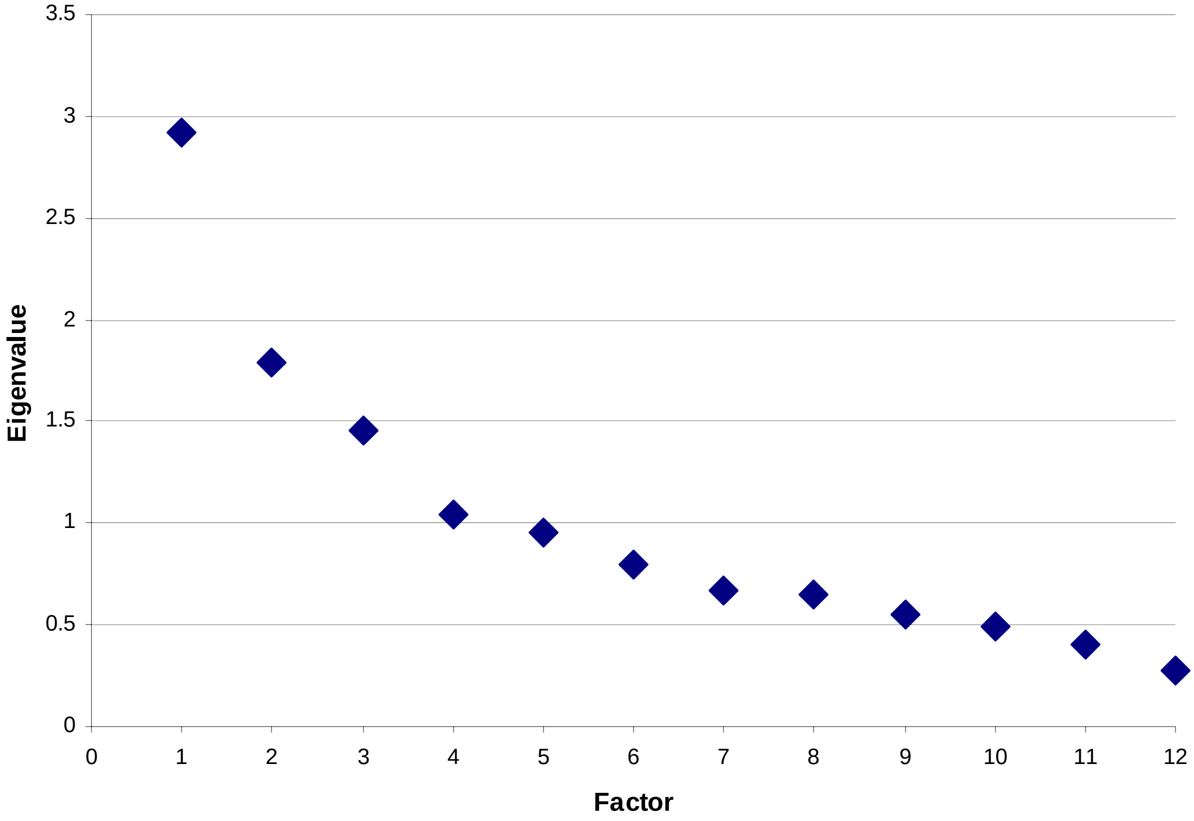
Appendix L – Kolmogorov-Smirnov Test for Normal Distribution on Latent Variables

Latent Variable	N	K-S Z	K-S D	Critical*
Credit Report Attitude	356	1.489	0.079	0.055
Check Registry Attitude	222	1.489	0.100	0.069
Monitor Accounts Attitude	356	8.148	0.432	0.055
Physical Security Attitude	356	2.403	0.127	0.055
Secure Password Attitude	356	3.045	0.161	0.055
Click on Link Attitude	356	1.744	0.092	0.055
Info Over Phone Attitude	356	2.814	0.149	0.055
Remember Password Attitude	356	1.449	0.077	0.055
Subjective Norm	356	4.686	0.248	0.055
Credit Report PBC	356	2.151	0.114	0.055
Check Registry PBC	222	1.461	0.098	0.069
Monitor Accounts PBC	356	6.072	0.322	0.055
Physical Security PBC	356	1.646	0.087	0.055
Secure Password PBC	356	3.342	0.177	0.055
Click on Link PBC	356	2.739	0.145	0.055
Info Over Phone PBC	356	3.192	0.169	0.055
Remember Password PBC	356	1.606	0.085	0.055
Credit Report Intention	356	1.862	0.099	0.055
Check Registry Intention	222	1.482	0.099	0.069
Monitor Accounts Intention	356	6.946	0.368	0.055
Physical Security Intention	356	3.750	0.199	0.055
Secure Password Intention	356	4.850	0.257	0.055
Click on Link Intention	356	2.925	0.155	0.055
Info Over Phone Intention	356	5.132	0.272	0.055
Remember Password Intention	356	3.150	0.167	0.055
Check Credit Report	356	5.151	0.273	0.055
Check Land Registry	356	7.775	0.412	0.055
Monitor Card and Bank Accounts	356	7.319	0.388	0.055
Use Physical Security	356	1.775	0.094	0.055
Use Secure Passwords	356	2.753	0.146	0.055
Click on Link in E-mail	356	4.670	0.248	0.055
Give Personal Info Over Phone	356	6.805	0.361	0.055
Use 'Remember Password'	356	3.918	0.208	0.055

* Critical value is for 0.01 level of significance

Appendix M – Principal Components Eigenvalues

Eigenvalues of the Correlation Matrix				
	Eigenvalue	Difference	Proportion	Cumulative
1	2.92062221	1.13095901	0.2434	0.2434
2	1.78966319	0.33627437	0.1491	0.3925
3	1.45338882	0.41095534	0.1211	0.5136
4	1.04243348	0.09151232	0.0869	0.6005
5	0.95092116	0.15129890	0.0792	0.6798
6	0.79962226	0.13091014	0.0666	0.7464
7	0.66871212	0.01986954	0.0557	0.8021
8	0.64884258	0.09659211	0.0541	0.8562
9	0.55225047	0.05945139	0.0460	0.9022
10	0.49279908	0.09090728	0.0411	0.9433
11	0.40189180	0.12303899	0.0335	0.9768
12	0.27885281		0.0232	1.0000



Scree Plot

Appendix N – Principal Components Pattern Matrix - Imputed Values

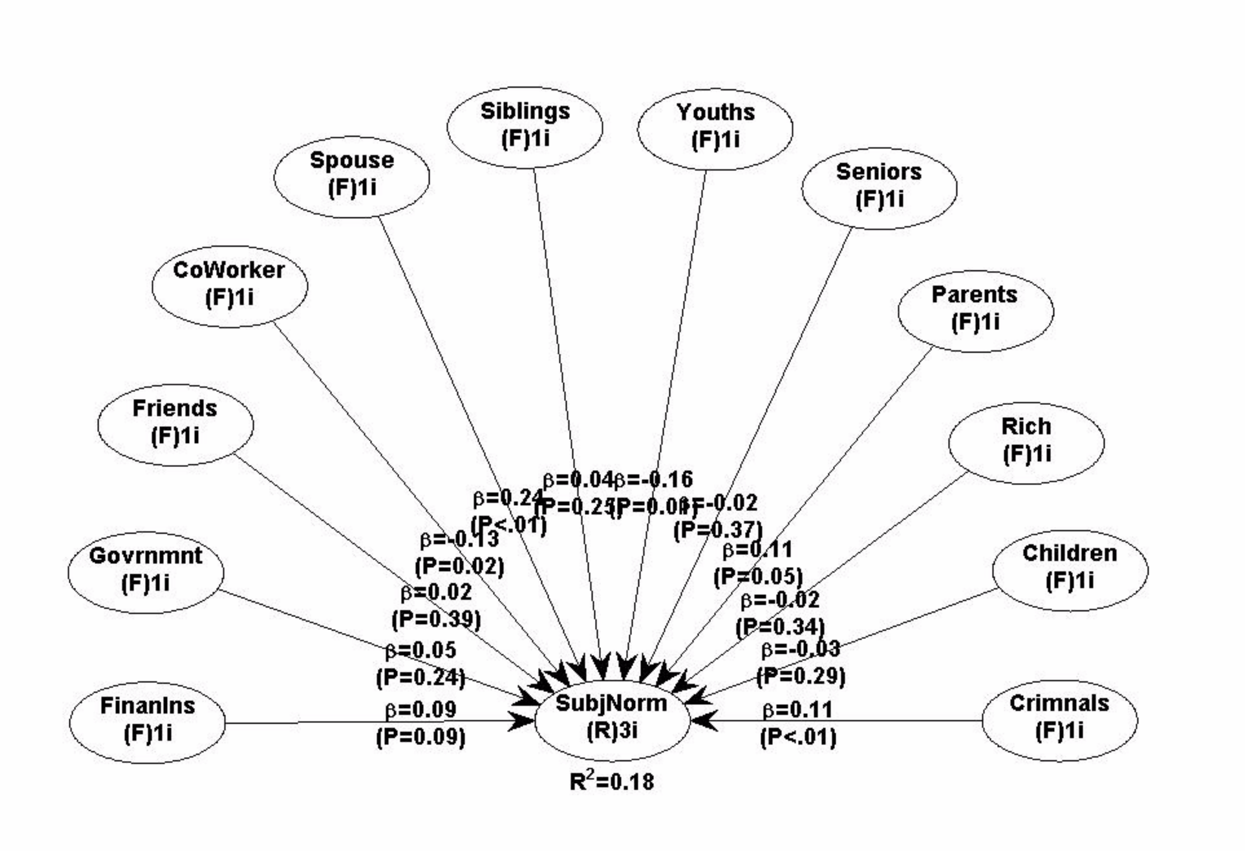
Imputed values for H04 (Check land registry office) when respondent did not own their home

		Factor 1	Factor 2	Factor 3	Factor 4	Factor 5
H06	Have different passwords	**.751**	.034	.126	.196	-.079
H08	Shred financial or important documents	**.716**	-.129	-.004	-.144	.186
H05	Use hard-to-break passwords	**.705**	.082	.159	.059	-.203
H09	Keep financial info in secure place	**.638**	.161	-.100	-.066	.310
H03	Request a copy of my credit report	-.057	**.885**	.092	-.043	-.035
H04	Check land registry office records	.066	**.827**	-.054	.080	.147
H02	Monitor bank account balances	.044	.023	**.892**	-.126	.007
H01	Monitor credit card accounts	.062	.033	**.891**	.001	.021
H12	Click on link in e-mail	.137	-.106	-.022	**.828**	.062
H11	Give personal information over the phone	-.073	.203	-.130	**.721**	-.101
H07	Use a locked mailbox for incoming mail	.142	.146	.019	-.067	**.793**
H10	Use "remember my password"	-.355	-.107	.203	.331	**.488**

Imputation was performed by the Multiple Imputation procedure of SAS version 8 using a single Markov Chain Monte Carlo method with 200 ‘burn in’ iterations and 100 iterations between each of five imputations. Input was all behavioural items (H01-H12) and demographic items(age, gender, language, number of bank accounts and credit cards, and whether the respondent had been a victim of credit card or other identity fraud). Initial values were derived using the expectation-maximization algorithm. Both upper and lower limit options were used to constrain the imputations to the possible values of the Lickert scale used in the item.

Appendix O – Subjective Norm Model

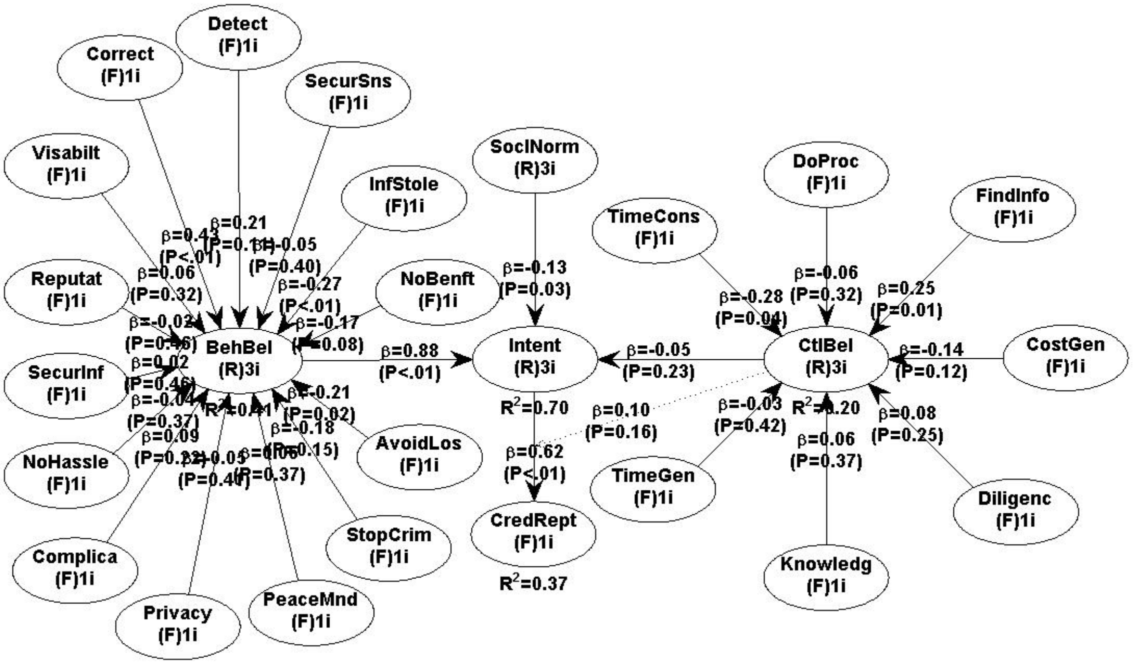
SubjNorm Most people whose opinions I value, would approve of my protecting my personal identity information



		Path	**P**	**Effect**
Variable	Description	**coefficients**	**Values**	**sizes**
FinanIns	Financial Institutions	0.088	0.085	0.012
Govrnmnt	Government	0.050	0.238	0.005
Friends	Friends	0.022	0.388	0.000
CoWorker	Co-Workers	-0.127	0.024	0.013
Spouse	Spouse	0.244	<0.001	0.076
Siblings	Brothers and sisters	0.039	0.252	0.006
Youths	Young people	-0.158	0.010	0.028
Seniors	Seniors	-0.023	0.370	0.002
Parents	Your parents	0.110	0.053	0.024
Rich	High net worth individuals	-0.023	0.341	0.002
Children	Your children	-0.035	0.287	0.002
Crimnals	Criminals	0.112	0.007	0.014
R Value		0.179		

Appendix P – Full TPB Models

CredRep I request a copy of my credit report at least once a year



Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to check credit report	0.623			
BehBel	Attitude towards getting credit report		0.883		
CtlBel	PBC towards getting my credit report		-0.053		
SoclNor	Subjective Norm		-0.131		
AvoidLo	Avoiding financial loss (g)			-0.209	
StopCri	Stopping criminal activity (g)			-0.176	
PeaceMn	Having peace of mind (g)			0.056	
Privacy	Protecting my privacy (g)			-0.045	
Complic	Complicating transactions (g)			0.092	
NoHassl	Avoiding the hassle of dealing with fraud (g)			-0.037	
SecurIn	Securing my personal information (g)			0.020	
Reputat	Preventing the loss of my reputation (g)			-0.016	
Visabil	Reducing my online visibility (g)			0.055	
Correct	Correct mistakes			0.430	
Detect	Detect unauthorized use			0.206	
SecurSn	Sense of security			-0.051	
InfStol	Report will be stolen			-0.275	
NoBenft	Get no benefit			-0.175	
TimeGen	Takes a lot of time (g)				-0.025
Knowled	Requires a lot of knowledge (g)				0.057

Diligen	Requires diligence (g)				0.083
CostGen	Costs a lot (g)				-0.144
FindInf	Can easily find out how				0.252
DoProc	Able to follow the process				-0.065
TimeCon	Have enough time				-0.280
CtlBel*	Moderation of Intent by PBC	0.103			

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to check credit report	<0.001			
BehBel	Attitude towards getting credit report		<0.001		
CtlBel	PBC towards getting my credit report		0.229		
SoclNor	Subjective Norm		0.028		
AvoidLo	Avoiding financial loss (g)			0.019	
StopCri	Stopping criminal activity (g)			0.145	
PeaceMn	Having peace of mind (g)			0.369	
Privacy	Protecting my privacy (g)			0.406	
Complic	Complicating transactions (g)			0.215	
NoHassl	Avoiding the hassle of dealing with fraud (g)			0.375	
SecurIn	Securing my personal information (g)			0.455	
Reputat	Preventing the loss of my reputation (g)			0.457	
Visabil	Reducing my online visibility (g)			0.318	
Correct	Correct mistakes			0.002	
Detect	Detect unauthorized use			0.108	
SecurSn	Sense of security			0.402	
InfStol	Report will be stolen			0.006	
NoBenft	Get no benefit			0.082	
TimeGen	Takes a lot of time (g)				0.422
Knowled	Requires a lot of knowledge (g)				0.369
Diligen	Requires diligence (g)				0.248
CostGen	Costs a lot (g)				0.121
FindInf	Can easily find out how				0.014
DoProc	Able to follow the process				0.318
TimeCon	Have enough time				0.040
CtlBel*	Moderation of Intent by PBC	0.156			

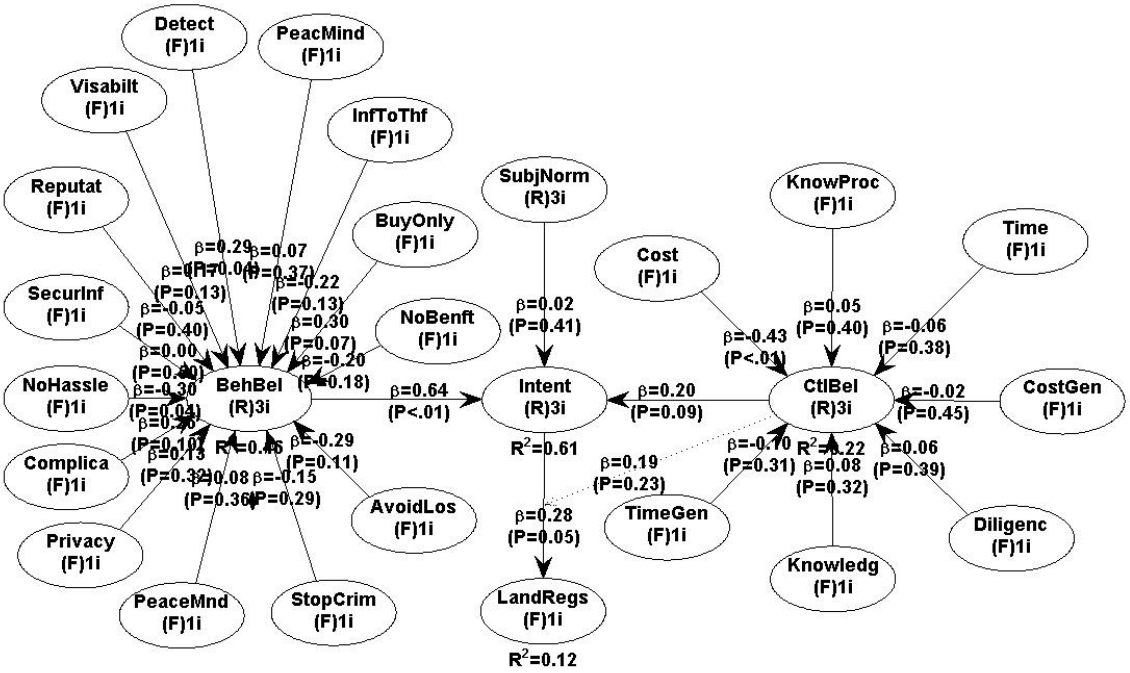
Effect Size

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to check credit report	0.375			
BehBel	Attitude towards getting credit report		0.726		
CtlBel	PBC towards getting my credit report		0.014		
SoclNor	Subjective Norm		0.014		
AvoidLo	Avoiding financial loss (g)			0.006	
StopCri	Stopping criminal activity (g)			0.004	
PeaceMn	Having peace of mind (g)			0.006	
Privacy	Protecting my privacy (g)			0.008	
Complic	Complicating transactions (g)			0.011	
NoHassl	Avoiding the hassle of dealing with fraud (g)			0.000	
SecurIn	Securing my personal information (g)			0.004	

Reputat	Preventing the loss of my reputation (g)			0.001	
Visabil	Reducing my online visibility (g)			0.002	
Correct	Correct mistakes			0.186	
Detect	Detect unauthorized use			0.075	
SecurSn	Sense of security			0.017	
InfStol	Report will be stolen			0.064	
NoBenft	Get no benefit			0.076	
TimeGen	Takes a lot of time (g)				0.001
Knowled	Requires a lot of knowledge (g)				0.003
Diligen	Requires diligence (g)				0.007
CostGen	Costs a lot (g)				0.037
FindInf	Can easily find out how				0.049
DoProc	Able to follow the process				0.018
TimeCon	Have enough time				0.084
CtlBel*	Moderation of Intent by PBC	0.003			
		Behaviour	Intention	Attitude	PBC
R Squared		0.372	0.698	0.408	0.200

(g) General beliefs - all others are specific to the behaviour

LandReg Check land registry office records at least once a year



Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to check with land registry office	0.275			
CtlBel	PBC towards checking land registry office		0.197		
BehBel	Attitude towards checking land registry office		0.645		
SubjNorm	Subjective Norm		0.020		
AvoidLos	Avoiding financial loss (g)			-0.290	
StopCrim	Stopping criminal activity (g)			-0.152	
PeaceMnd	Having peace of mind (g)			0.085	
Privacy	Protecting my privacy (g)			0.130	
Complica	Complicating transactions (g)			0.255	
NoHassle	Avoiding the hassle of dealing with fraud (g)			-0.299	
SecurInf	Securing my personal information (g)			0.003	
Reputat	Preventing the loss of my reputation (g)			-0.050	
Visabilt	Reducing my online visibility (g)			0.175	
Detect	Detect any unauthorized mortgage			0.286	
PeacMind	Have peace of mind			0.068	
InfToThf	Source of information to identity thieves			-0.217	
BuyOnly	Only needed when buying or selling			0.296	
NoBenft	Will receive no benefit			-0.204	
TimeGen	Takes a lot of time (g)				-0.097
Knowledg	Requires a lot of knowledge (g)				0.077
Diligenc	Requires diligence (g)				0.055
CostGen	Costs a lot (g)				-0.021

Time	Time consuming				-0.060
KnowPro	Requires knowing the procedure				0.046
Cost	Costly				-0.434
CtlBel*	Moderation of Intent by PBC	0.187			

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to check with land registry office	0.052			
CtlBel	PBC towards checking land registry office		0.092		
BehBel	Attitude towards checking land registry office		<0.001		
SubjNorm	Subjective Norm		0.406		
AvoidLos	Avoiding financial loss (g)			0.112	
StopCrim	Stopping criminal activity (g)			0.292	
PeaceMnd	Having peace of mind (g)			0.359	
Privacy	Protecting my privacy (g)			0.316	
Complica	Complicating transactions (g)			0.100	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.044	
SecurInf	Securing my personal information (g)			0.495	
Reputat	Preventing the loss of my reputation (g)			0.396	
Visabilt	Reducing my online visibility (g)			0.129	
Detect	Detect any unauthorized mortgage			0.039	
PeacMind	Have peace of mind			0.365	
InfToThf	Source of information to identity thieves			0.130	
BuyOnly	Only needed when buying or selling			0.072	
NoBenft	Will receive no benefit			0.180	
TimeGen	Takes a lot of time (g)				0.310
Knowledg	Requires a lot of knowledge (g)				0.322
Diligenc	Requires diligence (g)				0.392
CostGen	Costs a lot (g)				0.453
Time	Time consuming				0.378
KnowPro	Requires knowing the procedure				0.397
Cost	Costly				0.006
CtlBel*	Moderation of Intent by PBC	0.232			

Effect Size

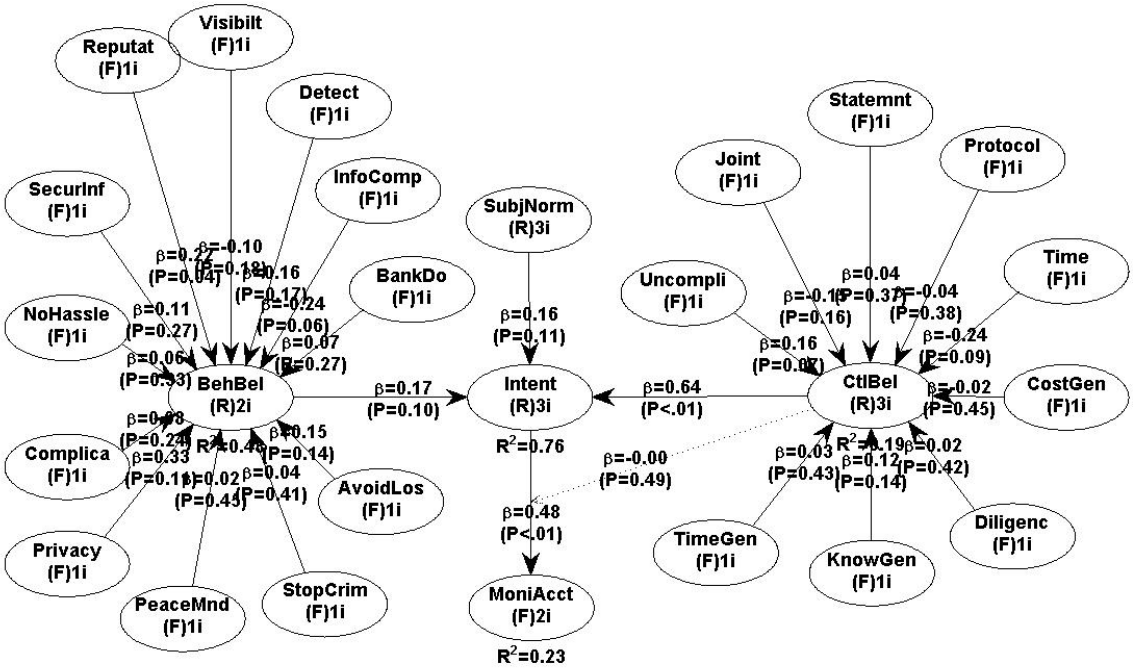
Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to check with land registry office	0.080			
CtlBel	PBC towards checking land registry office		0.115		
BehBel	Attitude towards checking land registry office		0.493		
SubjNorm	Subjective Norm		0.005		
AvoidLos	Avoiding financial loss (g)			0.050	
StopCrim	Stopping criminal activity (g)			0.014	
PeaceMnd	Having peace of mind (g)			0.001	
Privacy	Protecting my privacy (g)			0.016	
Complica	Complicating transactions (g)			0.015	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.044	
SecurInf	Securing my personal information (g)			0.000	

Reputat	Preventing the loss of my reputation (g)			0.002	
Visabilt	Reducing my online visibility (g)			0.016	
Detect	Detect any unauthorized mortgage			0.080	
PeacMind	Have peace of mind			0.015	
InfToThf	Source of information to identity thieves			0.065	
BuyOnly	Only needed when buying or selling			0.046	
NoBenft	Will receive no benefit			0.090	
TimeGen	Takes a lot of time (g)				0.002
Knowledg	Requires a lot of knowledge (g)				0.002
Diligenc	Requires diligence (g)				0.001
CostGen	Costs a lot (g)				0.004
Time	Time consuming				0.013
KnowPro	Requires knowing the procedure				0.004
Cost	Costly				0.195
CtlBel*	Moderation of Intent by PBC	0.039			
		Behaviou	Intentio		
		r	n	Attitude	PBC
R Squared		0.118	0.613	0.456	0.215

(g) General beliefs - all others are specific to the behaviour

MoniAcct Monitor Accounts

I monitor credit card accounts and activity at least once a month
I monitor bank account balances and activity at least once a month



Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to monitor bank accounts and credit cards	0.480			
BehBel	Attitude towards monitoring accounts and cards		0.174		
CtlBel	PBC towards monitoring accounts and cards		0.636		
SubjNorm	Subjective Norm		0.165		
AvoidLos	Avoiding financial loss (g)			0.149	
StopCrim	Stopping criminal activity (g)			0.042	
PeaceMnd	Having peace of mind (g)			0.025	
Privacy	Protecting my privacy (g)			0.332	
Complica	Complicating transactions (g)			0.077	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.061	
SecurInf	Securing my personal information (g)			0.112	
Reputat	Preventing the loss of my reputation (g)			0.217	
Visabilt	Reducing my online visibility (g)			-0.099	
Detect	Detect unauthorized use			0.158	
InfoComp	Banking information will be stored on my computer			-0.244	
BankDo	Bank will do it			0.072	
TimeGen	Takes a lot of time (g)				0.029
Knowledg	Requires a lot of knowledge (g)				0.124
Diligenc	Requires diligence (g)				0.023

CostGen	Costs a lot (g)				-0.016
Time	Takes too much time				-0.245
Protocol	Uses elaborate online security protocols				-0.045
Statemnt	Needs regular statements				0.041
Joint	Difficult if jointly owned				-0.152
Uncompli	Easier if process is uncomplicated				0.161
CtlBel*Intent	Moderation of Intent by PBC	-0.003			

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to monitor bank accounts and credit cards	0.005			
BehBel	Attitude towards monitoring accounts and cards		0.105		
CtlBel	PBC towards monitoring accounts and cards		<0.001		
SubjNorm	Subjective Norm		0.113		
AvoidLos	Avoiding financial loss (g)			0.142	
StopCrim	Stopping criminal activity (g)			0.406	
PeaceMnd	Having peace of mind (g)			0.453	
Privacy	Protecting my privacy (g)			0.107	
Complica	Complicating transactions (g)			0.238	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.327	
SecurInf	Securing my personal information (g)			0.268	
Reputat	Preventing the loss of my reputation (g)			0.039	
Visabilt	Reducing my online visibility (g)			0.181	
Detect	Detect unauthorized use			0.169	
InfoComp	Banking information will be stored on my computer			0.063	
BankDo	Bank will do it			0.271	
TimeGen	Takes a lot of time (g)				0.430
Knowledg	Requires a lot of knowledge (g)				0.144
Diligenc	Requires diligence (g)				0.421
CostGen	Costs a lot (g)				0.452
Time	Takes too much time				0.089
Protocol	Uses elaborate online security protocols				0.380
Statemnt	Needs regular statements				0.366
Joint	Difficult if jointly owned				0.160
Uncompli	Easier if process is uncomplicated				0.066
CtlBel*Intent	Moderation of Intent by PBC	0.495			

Effect Sizes

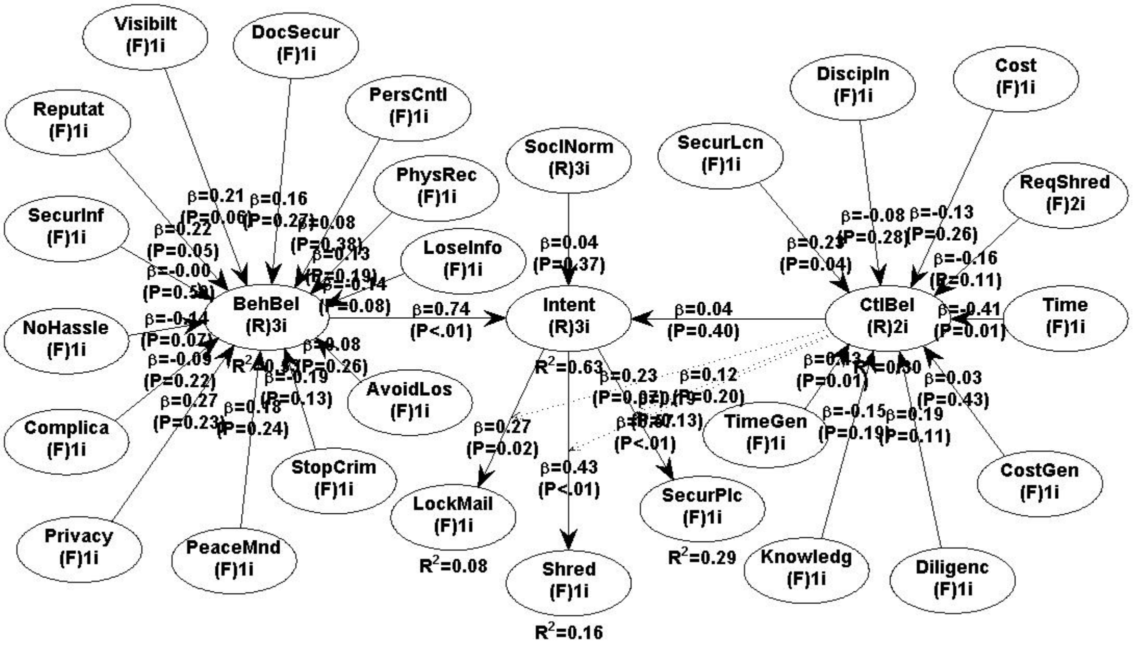
Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intent to monitor bank accounts and credit cards	0.232			
BehBel	Attitude towards monitoring accounts and cards		0.126		
CtlBel	PBC towards monitoring accounts and cards		0.539		
SubjNorm	Subjective Norm		0.095		
AvoidLos	Avoiding financial loss (g)			0.051	
StopCrim	Stopping criminal activity (g)			0.014	
PeaceMnd	Having peace of mind (g)			0.011	
Privacy	Protecting my privacy (g)			0.192	
Complica	Complicating transactions (g)			0.007	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.012	

SecurInf	Securing my personal information (g)			0.055	
Reputat	Preventing the loss of my reputation (g)			0.033	
Visabilt	Reducing my online visibility (g)			0.020	
Detect	Detect unauthorized use			0.066	
InfoComp	Banking information will be stored on my computer			0.039	
BankDo	Bank will do it			0.016	
TimeGen	Takes a lot of time (g)				0.001
Knowledg	Requires a lot of knowledge (g)				0.017
Diligenc	Requires diligence (g)				0.000
CostGen	Costs a lot (g)				0.002
Time	Takes too much time				0.081
Protocol	Uses elaborate online security protocols				0.009
Statemnt	Needs regular statements				0.002
Joint	Difficult if jointly owned				0.044
Uncompli	Easier if process is uncomplicated				0.031
CtlBel*Intent	Moderation of Intent by PBC	0.001			
		Behaviou	Intentio		
		r	n	Attitude	PBC
R Squared		0.233	0.760	0.477	0.186

(g) General beliefs - all others are specific to the behaviour

Physical Security

LockMail	I use a locked mailbox for incoming mail
Shred	I shred financial or important documents before discarding them
SecurPlc	I keep sensitive financial information in a secure location



Path Coefficients

Variable	Description	LockMail	Shred	SecurPlc	Intention	Attitude	PBC
Intent	Intend to secure my documents	0.274	0.431	0.575			
BehBel	Attitude to securing documents				0.742		
CtlBel	PBC of securing documents				0.036		
SoclNorm	Subjective Norm				0.045		
AvoidLos	Avoiding financial loss (g)					0.085	
StopCrim	Stopping criminal activity (g)					-0.190	
PeaceMnd	Having peace of mind (g)					0.180	
Privacy	Protecting my privacy (g)					0.274	
Complica	Complicating transactions (g)					-0.094	
NoHassle	Avoiding the hassle of fraud (g)					-0.141	
SecurInf	Securing personal info (g)					-0.002	
Reputat	Preventing loss of reputation (g)					0.222	
Visibilt	Reducing my online visibility (g)					0.207	
DocSecur	My identity info will be secure					0.165	
PersCntl	Maintain personal control					0.083	
PhysRec	Have a physical record					0.131	
LoseInfo	Lose my personal identity info					-0.140	

TimeGen	Takes a lot of time (g)						0.428
Knowledg	Requires a lot of knowledge (g)						-0.148
Diligenc	Requires diligence (g)						0.185
CostGen	Costs a lot (g)						0.026
Time	Takes too much time						-0.409
ReqShred	Requires a shredder						-0.156
Cost	Is expensive						-0.129
Discipln	Requires discipline						-0.079
SecurLcn	Requires a secure location						0.234
CtlBel*Intent	Moderation of Intent by PBC	0.232	0.190	0.116			

P Values

Variable	Description	LockMail	Shred	SecurPlc	Intention	Attitude	PBC
Intent	Intend to secure my documents	0.020	<0.001	<0.001			
BehBel	Attitude to securing documents				<0.001		
CtlBel	PBC of securing documents				0.400		
SoclNorm	Subjective Norm				0.375		
AvoidLos	Avoiding financial loss (g)					0.259	
StopCrim	Stopping criminal activity (g)					0.135	
PeaceMnd	Having peace of mind (g)					0.241	
Privacy	Protecting my privacy (g)					0.228	
Complica	Complicating transactions (g)					0.224	
NoHassle	Avoiding the hassle of fraud (g)					0.066	
SecurInf	Securing personal info (g)					0.497	
Reputat	Preventing loss of reputation (g)					0.046	
Visibilt	Reducing my online visibility (g)					0.064	
DocSecur	My identity info will be secure					0.270	
PersCntl	Maintain personal control					0.382	
PhysRec	Have a physical record					0.189	
LoseInfo	Lose my personal identity info					0.079	
TimeGen	Takes a lot of time (g)						0.011
Knowledg	Requires a lot of knowledge (g)						0.191
Diligenc	Requires diligence (g)						0.107
CostGen	Costs a lot (g)						0.431
Time	Takes too much time						0.015
ReqShred	Requires a shredder						0.109
Cost	Is expensive						0.264
Discipln	Requires discipline						0.284
SecurLcn	Requires a secure location						0.038
CtlBel*Intent	Moderation of Intent by PBC	0.068	0.132	0.195			

Effect Size

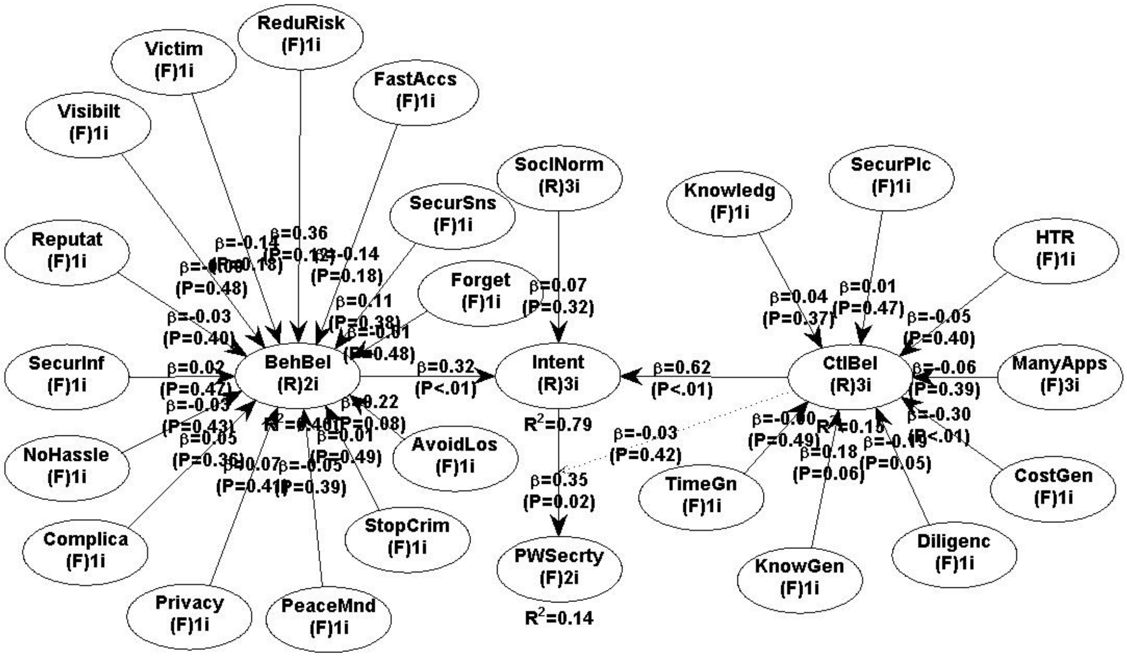
Variable	Description	LockMail	Shred	SecurPlc	Intention	Attitude	PBC
Intent	Intend to secure my documents	0.051	0.155	0.306			
BehBel	Attitude to securing documents				0.588		
CtlBel	PBC of securing documents				0.016		
SoclNorm	Subjective Norm				0.025		
AvoidLos	Avoiding financial loss (g)					0.034	

StopCrim	Stopping criminal activity (g)					0.059	
PeaceMnd	Having peace of mind (g)					0.093	
Privacy	Protecting my privacy (g)					0.153	
Complica	Complicating transactions (g)					0.017	
NoHassle	Avoiding the hassle of fraud (g)					0.003	
SecurInf	Securing personal info (g)					0.001	
Reputat	Preventing loss of reputation (g)					0.031	
Visibilt	Reducing my online visibility (g)					0.065	
DocSecur	My identity info will be secure					0.087	
PersCntl	Maintain personal control					0.037	
PhysRec	Have a physical record					0.053	
LoseInfo	Lose my personal identity info					0.017	
TimeGen	Takes a lot of time (g)						0.090
Knowledg	Requires a lot of knowledge (g)						0.031
Diligenc	Requires diligence (g)						0.004
CostGen	Costs a lot (g)						0.001
Time	Takes too much time						0.140
ReqShred	Requires a shredder						0.008
Cost	Is expensive						0.026
Discipln	Requires discipline						0.008
SecurLcn	Requires a secure location						0.075
CtlBel*Intent	Moderation of Intent by PBC	0.030	0.005	0.011			
		LockMail	Shred	SecurPlc	Intention	Attitude	PBC
R Squared		0.081	0.161	0.294	0.629	0.531	0.304

(g) General beliefs - all others are specific to the behaviour

PWSecrty Practice password security

I use hard-to-break passwords
I use different passwords for different applications



Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to use secure passwords	0.355			
CtlBel	PBC to using secure passwords		0.621		
SubjNorm	Subjective Norm		0.066		
BehBel	Attitude towards using secure passwords		0.318		
AvoidLos	Avoiding financial loss (g)			0.223	
StopCrim	Stopping criminal activity (g)			0.005	
PeaceMnd	Having peace of mind (g)			-0.048	
Privacy	Protecting my privacy (g)			0.070	
Complica	Complicating transactions (g)			0.053	
NoHassle	Avoiding the hassle of dealing with fraud (g)			-0.025	
SecurInf	Securing my personal information (g)			0.022	
Reputat	Preventing the loss of my reputation (g)			-0.034	
Visabilt	Reducing my online visibility (g)			-0.005	
Victim	Will be the victim of identity crime (n)			-0.143	
ReduRisk	Reduce the risk of identity crime			0.355	
FastAccs	Online access will be slower			-0.143	
SecurSns	Have a sense of security			0.111	
Forget	Will forget it			-0.005	
TimeGen	Takes a lot of time (g)				-0.004

KnowGen	Requires a lot of knowledge (g)				0.183
Diligenc	Requires diligence (g)				-0.189
CostGen	Costs a lot (g)				-0.298
ManyApps	Too many applications with different passwords				-0.056
HTR	Hard to remember*				-0.050
SecurPlc	Secure place to store my passwords				0.008
Knowledg	Need to know what a secure password is				0.036
CtlBel*Intent	Moderation of Intent by PBC	-0.026			

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to use secure passwords	0.022			
CtlBel	PBC towards getting my credit report		<0.001		
SubjNorm	Subjective Norm		0.318		
BehBel	Attitude towards getting credit report		0.010		
AvoidLos	Avoiding financial loss (g)			0.082	
StopCrim	Stopping criminal activity (g)			0.487	
PeaceMnd	Having peace of mind (g)			0.391	
Privacy	Protecting my privacy (g)			0.410	
Complica	Complicating transactions (g)			0.355	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.428	
SecurInf	Securing my personal information (g)			0.467	
Reputat	Preventing the loss of my reputation (g)			0.397	
Visabilt	Reducing my online visibility (g)			0.484	
Victim	Will be the victim of identity crime (n)			0.179	
ReduRisk	Reduce the risk of identity crime			0.123	
FastAccs	Online access will be slower			0.181	
SecurSns	Have a sense of security			0.379	
Forget	Will forget it			0.483	
TimeGen	Takes a lot of time (g)				0.487
KnowGen	Requires a lot of knowledge (g)				0.058
Diligenc	Requires diligence (g)				0.046
CostGen	Costs a lot (g)				0.008
ManyApps	Too many applications with different passwords				0.394
HTR	Hard to remember*				0.403
SecurPlc	Secure place to store my passwords				0.474
Knowledg	Need to know what a secure password is				0.372
CtlBel*Intent	Moderation of Intent by PBC	0.425			

Effect Size

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to use secure passwords	0.132			
CtlBel	PBC towards getting my credit report		0.523		
SubjNorm	Subjective Norm		0.036		
BehBel	Attitude towards getting credit report		0.226		
AvoidLos	Avoiding financial loss (g)			0.108	
StopCrim	Stopping criminal activity (g)			0.002	
PeaceMnd	Having peace of mind (g)			0.019	
Privacy	Protecting my privacy (g)			0.032	

Complica	Complicating transactions (g)			0.003	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.003	
SecurInf	Securing my personal information (g)			0.011	
Reputat	Preventing the loss of my reputation (g)			0.001	
Visabilt	Reducing my online visibility (g)			0.001	
Victim	Will be the victim of identity crime (n)			0.070	
ReduRisk	Reduce the risk of identity crime			0.201	
FastAccs	Online access will be slower			0.004	
SecurSns	Have a sense of security			0.064	
Forget	Will forget it			0.001	
TimeGen	Takes a lot of time (g)				0.000
KnowGen	Requires a lot of knowledge (g)				0.011
Diligenc	Requires diligence (g)				0.041
CostGen	Costs a lot (g)				0.088
ManyApps	Too many applications with different passwords				0.006
HTR	Hard to remember*				0.007
SecurPlc	Secure place to store my passwords				0.000
Knowledg	Need to know what a secure password is				0.002
CtlBel*Intent	Moderation of Intent by PBC	0.007			
		Behaviour	Intention	Attitude	PBC
R Squared		0.139	0.785	0.465	0.155

(g) General beliefs - all others are specific to the behaviour

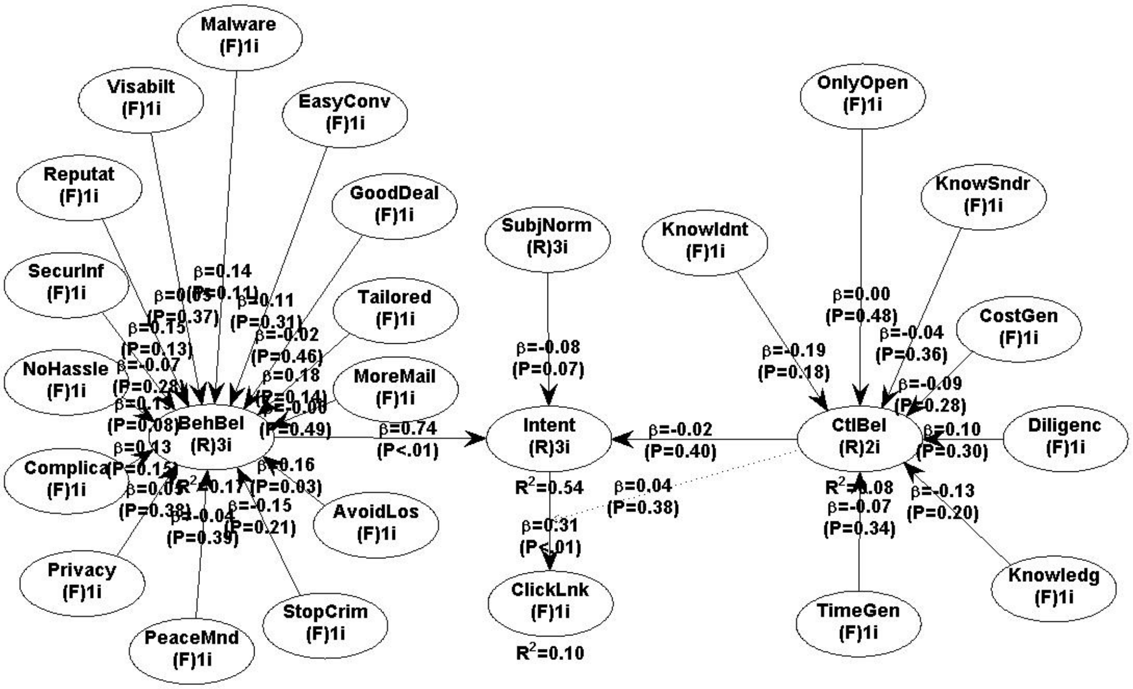
* Combined items due to multicolinearity

Frequently changing my passwords makes them difficult to remember

Differing password standards in different applications make remembering passwords difficult

Secure passwords are hard to remember

ClickLnk I respond to a business by clicking on a link in an e-mail



Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to click on a link in an e-mail	0.310			
BehBel	Attitude towards clicking on a link		0.743		
CtlBel	PBC towards clicking on a link		-0.018		
SubjNorm	Subjective Norm		-0.084		
AvoidLos	Avoiding financial loss (g)			0.158	
StopCrim	Stopping criminal activity (g)			-0.150	
PeaceMnd	Having peace of mind (g)			-0.040	
Privacy	Protecting my privacy (g)			0.055	
Complica	Complicating transactions (g)			0.127	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.194	
SecurInf	Securing my personal information (g)			-0.072	
Reputat	Preventing the loss of my reputation (g)			0.151	
Visabilt	Reducing my online visibility (g)			0.047	
Malware	Will be the victim of malware			0.139	
EasyConv	Easy and convenient			0.106	
GoodDeal	Will get a good deal			-0.016	
Tailored	Get information tailored to me			0.176	
MoreMail	Get more e-mail from the same source			-0.003	
TimeGen	Takes a lot of time (g)				-0.073
Knowledg	Requires a lot of knowledge (g)				-0.134
Diligenc	Requires diligence (g)				0.095

CostGen	Costs a lot (g)				-0.087
KnowSndr	Knowing the sender reduces the risk				-0.045
OnlyOpen	Will not be the victim if I just open and close				0.005
KnowIdnt	Difficult to know the true identity of the sender				-0.187
CtlBel*Intent	Moderation of intent by PBC	0.035			

P Values

		Behaviou	Intentio		
Variable	Description	r	n	Attitude	PBC
Intent	Intend to click on a link in an e-mail	0.008			
BehBel	Attitude towards clicking on a link		<0.001		
CtlBel	PBC towards clicking on a link		0.400		
SubjNorm	Subjective Norm		0.073		
AvoidLos	Avoiding financial loss (g)			0.034	
StopCrim	Stopping criminal activity (g)			0.210	
PeaceMnd	Having peace of mind (g)			0.390	
Privacy	Protecting my privacy (g)			0.375	
Complica	Complicating transactions (g)			0.147	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.079	
SecurInf	Securing my personal information (g)			0.278	
Reputat	Preventing the loss of my reputation (g)			0.129	
Visabilt	Reducing my online visibility (g)			0.369	
Malware	Will be the victim of malware			0.115	
EasyConv	Easy and convenient			0.311	
GoodDeal	Will get a good deal			0.455	
Tailored	Get information tailored to me			0.136	
MoreMail	Get more e-mail from the same source			0.495	
TimeGen	Takes a lot of time (g)				0.337
Knowledg	Requires a lot of knowledge (g)				0.204
Diligenc	Requires diligence (g)				0.304
CostGen	Costs a lot (g)				0.279
KnowSndr	Knowing the sender reduces the risk				0.361
OnlyOpen	Will not be the victim if I just open and close				0.485
KnowIdnt	Difficult to know the true identity of the sender				0.181
CtlBel*Intent	Moderation of intent by PBC	0.384			

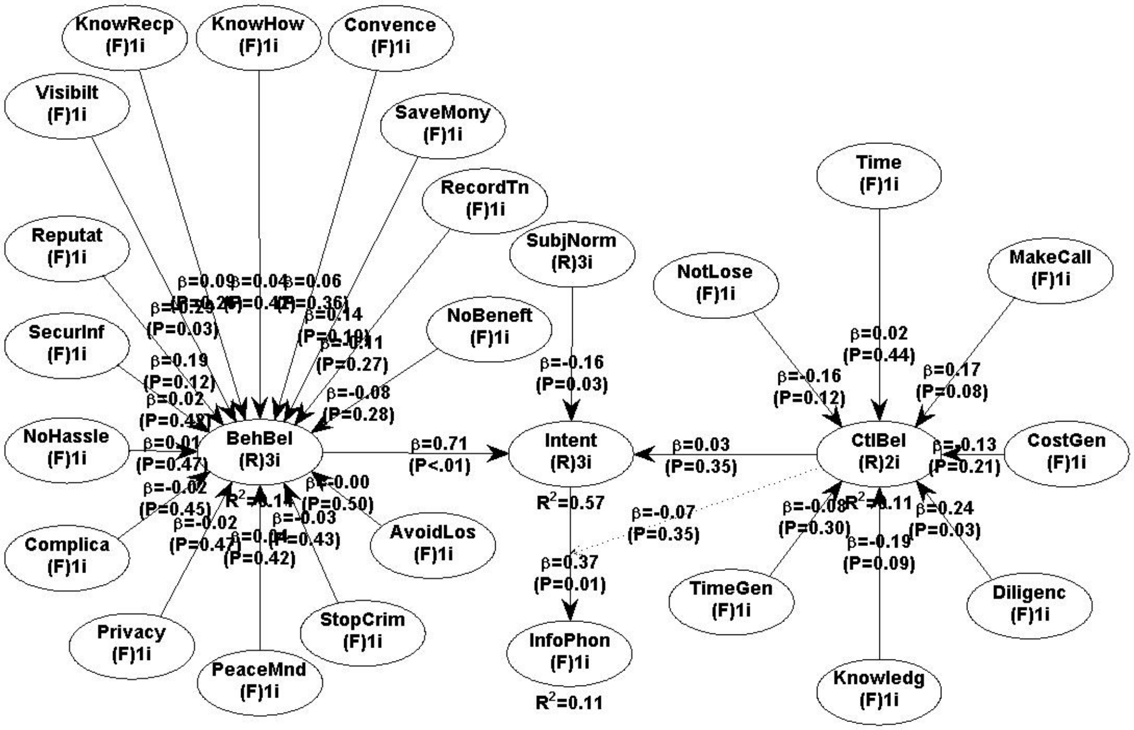
Effect Size

		Behaviou	Intentio		
Variable	Description	r	n	Attitude	PBC
Intent	Intend to click on a link in an e-mail	0.097			
BehBel	Attitude towards clicking on a link		0.543		
CtlBel	PBC towards clicking on a link		0.005		
SubjNorm	Subjective Norm		0.003		
AvoidLos	Avoiding financial loss (g)			0.013	
StopCrim	Stopping criminal activity (g)			0.019	
PeaceMnd	Having peace of mind (g)			0.004	
Privacy	Protecting my privacy (g)			0.001	
Complica	Complicating transactions (g)			0.002	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.037	
SecurInf	Securing my personal information (g)			0.000	
Reputat	Preventing the loss of my reputation (g)			0.024	

Visabilt	Reducing my online visibility (g)			0.000	
Malware	Will be the victim of malware			0.018	
EasyConv	Easy and convenient			0.016	
GoodDeal	Will get a good deal			0.002	
Tailored	Get information tailored to me			0.037	
MoreMail	Get more e-mail from the same source			0.000	
TimeGen	Takes a lot of time (g)				0.008
Knowledg	Requires a lot of knowledge (g)				0.020
Diligenc	Requires diligence (g)				0.007
CostGen	Costs a lot (g)				0.010
KnowSndr	Knowing the sender reduces the risk				0.005
OnlyOpen	Will not be the victim if I just open and close				0.000
KnowIdnt	Difficult to know the true identity of the sender				0.035
CtlBel*Intent	Moderation of intent by PBC	0.002			
		Behaviour	Intention	Attitude	PBC
R Squared		0.098	0.541	0.167	0.085

(g) General beliefs - all others are specific to the behaviour

InfoPho I give personal information over the phone



Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to give personal information over the phone	0.370			
BehBel	Attitude to giving personal info over the phone		0.709		
CtlBel	PBC towards giving personal info over the phone		0.033		
SubjNorm	Subjective Norm		-0.156		
AvoidLos	Avoiding financial loss (g)			0.000	
StopCrim	Stopping criminal activity (g)			-0.034	
PeaceMnd	Having peace of mind (g)			0.035	
Privacy	Protecting my privacy (g)			-0.016	
Complica	Complicating transactions (g)			-0.020	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.015	
SecurInf	Securing my personal information (g)			0.023	
Reputat	Preventing the loss of my reputation (g)			0.192	
Visabilt	Reducing my online visibility (g)			-0.288	
KnowRec	Do not really know who the person is			0.092	
KnowHow	Information may be used in other ways			0.040	
Convenc	Easy and convenient			0.063	
SaveMon	Get a good deal			0.137	
RecordTn	Have a record of the conversation			-0.108	
NoBeneft	Will receive no benefit			-0.075	
TimeGen	Takes a lot of time (g)				-0.084
Knowledg	Requires a lot of knowledge (g)				-0.191

Diligenc	Requires diligence (g)				0.237
CostGen	Costs a lot (g)				-0.128
MakeCall	Only if I make the call				0.172
Time	Takes too much time				0.019
NotLose	Will lose nothing				-0.160
CtlBel*Intent	Moderation of intent by PBC	-0.072			

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to give personal information over the phone	0.013			
BehBel	Attitude to giving personal info over the phone		<0.001		
CtlBel	PBC towards giving personal info over the phone		0.345		
SubjNorm	Subjective Norm		0.029		
AvoidLos	Avoiding financial loss (g)			0.499	
StopCrim	Stopping criminal activity (g)			0.435	
PeaceMnd	Having peace of mind (g)			0.421	
Privacy	Protecting my privacy (g)			0.471	
Complica	Complicating transactions (g)			0.446	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.465	
SecurInf	Securing my personal information (g)			0.415	
Reputat	Preventing the loss of my reputation (g)			0.119	
Visabilt	Reducing my online visibility (g)			0.025	
KnowRec	Do not really know who the person is			0.263	
KnowHow	Information may be used in other ways			0.420	
Convenc	Easy and convenient			0.365	
SaveMon	Get a good deal			0.187	
RecordTn	Have a record of the conversation			0.266	
NoBeneft	Will receive no benefit			0.281	
TimeGen	Takes a lot of time (g)				0.296
Knowledg	Requires a lot of knowledge (g)				0.092
Diligenc	Requires diligence (g)				0.034
CostGen	Costs a lot (g)				0.206
MakeCall	Only if I make the call				0.084
Time	Takes too much time				0.442
NotLose	Will lose nothing				0.122
CtlBel*Intent	Moderation of intent by PBC	0.346			

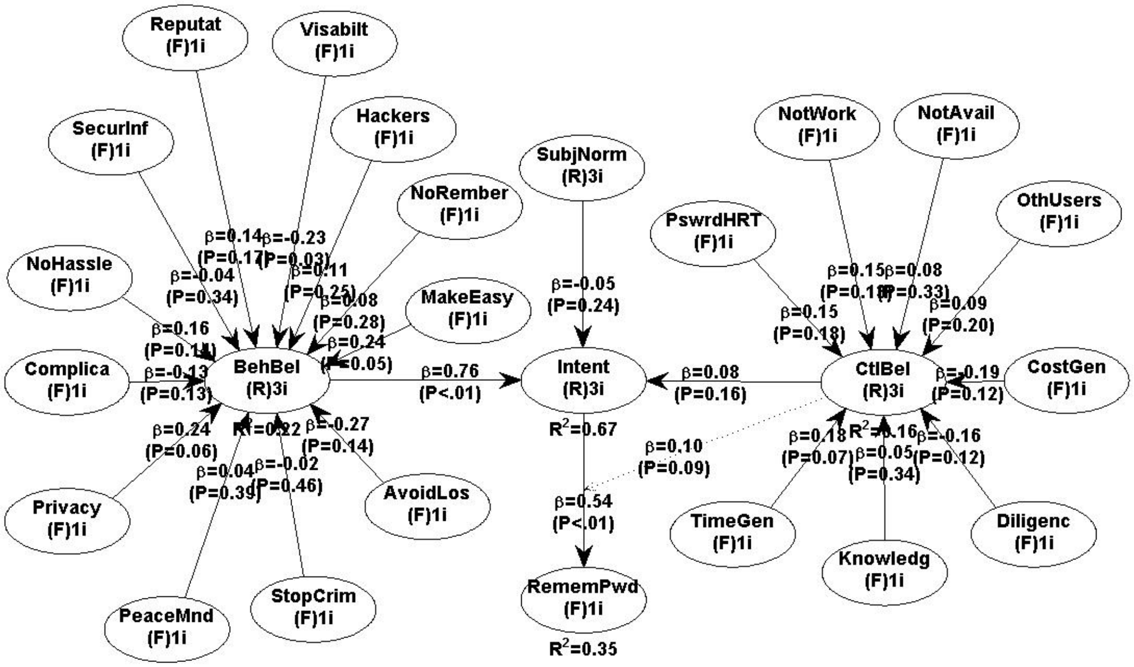
Effect Size

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to give personal information over the phone	0.123			
BehBel	Attitude to giving personal info over the phone		0.522		
CtlBel	PBC towards giving personal info over the phone		0.009		
SubjNorm	Subjective Norm		0.035		
AvoidLos	Avoiding financial loss (g)			0.000	
StopCrim	Stopping criminal activity (g)			0.004	
PeaceMnd	Having peace of mind (g)			0.004	
Privacy	Protecting my privacy (g)			0.002	
Complica	Complicating transactions (g)			0.001	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.000	

SecurInf	Securing my personal information (g)			0.002	
Reputat	Preventing the loss of my reputation (g)			0.029	
Visabilt	Reducing my online visibility (g)			0.063	
KnowRec	Do not really know who the person is			0.009	
KnowHow	Information may be used in other ways			0.002	
Convenc	Easy and convenient			0.007	
SaveMon	Get a good deal			0.024	
RecordTn	Have a record of the conversation			0.006	
NoBeneft	Will receive no benefit			0.001	
TimeGen	Takes a lot of time (g)				0.009
Knowledg	Requires a lot of knowledge (g)				0.035
Diligenc	Requires diligence (g)				0.027
CostGen	Costs a lot (g)				0.016
MakeCall	Only if I make the call				0.010
Time	Takes too much time				0.001
NotLose	Will lose nothing				0.017
CtlBel*Intent	Moderation of intent by PBC	0.009			
		Behaviour	Intention	Attitude	PBC
R Squared		0.115	0.567	0.142	0.114

(g) General beliefs - all others are specific to the behaviour

RememPwd I select “remember my card number” or "remember my password”



Path Coefficients

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to use "remember my password”	0.542			
BehBel	Attitude to using "remember my password”		0.761		
CtlBel	PBC toward using "remember my password”		0.081		
SubjNorm	Subjective Norm		-0.051		
AvoidLos	Avoiding financial loss (g)			-0.268	
StopCrim	Stopping criminal activity (g)			-0.020	
PeaceMnd	Having peace of mind (g)			0.042	
Privacy	Protecting my privacy (g)			0.244	
Complica	Complicating transactions (g)			-0.129	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.162	
SecurInf	Securing my personal information (g)			-0.040	
Reputat	Preventing the loss of my reputation (g)			0.139	
Visabilt	Reducing my online visibility (g)			-0.234	
Hackers	“Hackers” will find out my password			0.106	
NoRember	Will not need to remember passwords			0.082	
MakeEasy	Web sites are easier to use			0.238	
TimeGen	Takes a lot of time (g)				0.182
Knowledg	Requires a lot of knowledge (g)				0.050
Diligenc	Requires diligence (g)				-0.162
CostGen	Costs a lot (g)				-0.192
OthUser	Less secure if other people use my computer				0.087
NotAvail	Not always available				0.080
NotWork	Does not always work				0.147

PswrdHTR	Good passwords are hard to remember				0.146
CtlBel*Intent	Moderation of intent by PBC	0.102			

P Values

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to use "remember my password”	<0.001			
BehBel	Attitude to using "remember my password”		<0.001		
CtlBel	PBC toward using "remember my password”		0.162		
SubjNorm	Subjective Norm		0.240		
AvoidLos	Avoiding financial loss (g)			0.139	
StopCrim	Stopping criminal activity (g)			0.463	
PeaceMnd	Having peace of mind (g)			0.392	
Privacy	Protecting my privacy (g)			0.056	
Complica	Complicating transactions (g)			0.126	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.140	
SecurInf	Securing my personal information (g)			0.343	
Reputat	Preventing the loss of my reputation (g)			0.167	
Visabilt	Reducing my online visibility (g)			0.027	
Hackers	“Hackers” will find out my password			0.252	
NoRember	Will not need to remember passwords			0.280	
MakeEasy	Web sites are easier to use			0.047	
TimeGen	Takes a lot of time (g)				0.071
Knowledg	Requires a lot of knowledge (g)				0.343
Diligenc	Requires diligence (g)				0.117
CostGen	Costs a lot (g)				0.123
OthUser	Less secure if other people use my computer				0.201
NotAvail	Not always available				0.332
NotWork	Does not always work				0.133
PswrdHTR	Good passwords are hard to remember				0.176
CtlBel*Intent	Moderation of intent by PBC	0.094			

Effect Size

Variable	Description	Behaviour	Intention	Attitude	PBC
Intent	Intend to use "remember my password”	0.318			
BehBel	Attitude to using "remember my password”		0.619		
CtlBel	PBC toward using "remember my password”		0.039		
SubjNorm	Subjective Norm		0.010		
AvoidLos	Avoiding financial loss (g)			0.061	
StopCrim	Stopping criminal activity (g)			0.001	
PeaceMnd	Having peace of mind (g)			0.002	
Privacy	Protecting my privacy (g)			0.018	
Complica	Complicating transactions (g)			0.013	
NoHassle	Avoiding the hassle of dealing with fraud (g)			0.018	
SecurInf	Securing my personal information (g)			0.003	
Reputat	Preventing the loss of my reputation (g)			0.022	
Visabilt	Reducing my online visibility (g)			0.028	
Hackers	“Hackers” will find out my password			0.011	
NoRember	Will not need to remember passwords			0.011	
MakeEasy	Web sites are easier to use			0.040	

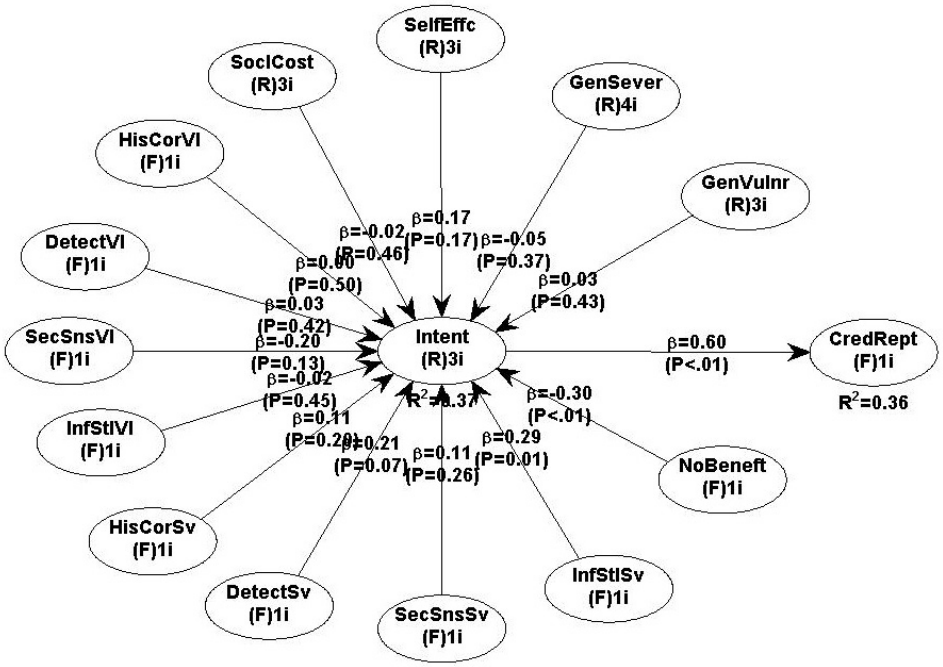
TimeGen	Takes a lot of time (g)				0.023
Knowledg	Requires a lot of knowledge (g)				0.003
Diligenc	Requires diligence (g)				0.025
CostGen	Costs a lot (g)				0.032
OthUser	Less secure if other people use my computer				0.011
NotAvail	Not always available				0.015
NotWork	Does not always work				0.033
PswrdHTR	Good passwords are hard to remember				0.017
CtlBel*Intent	Moderation of intent by PBC	0.034			

	Behaviour	Intention	Attitude	PBC
R Squared	0.352	0.667	0.218	0.159

(g) General beliefs - all others are specific to the behaviour

Appendix Q – PMT Models

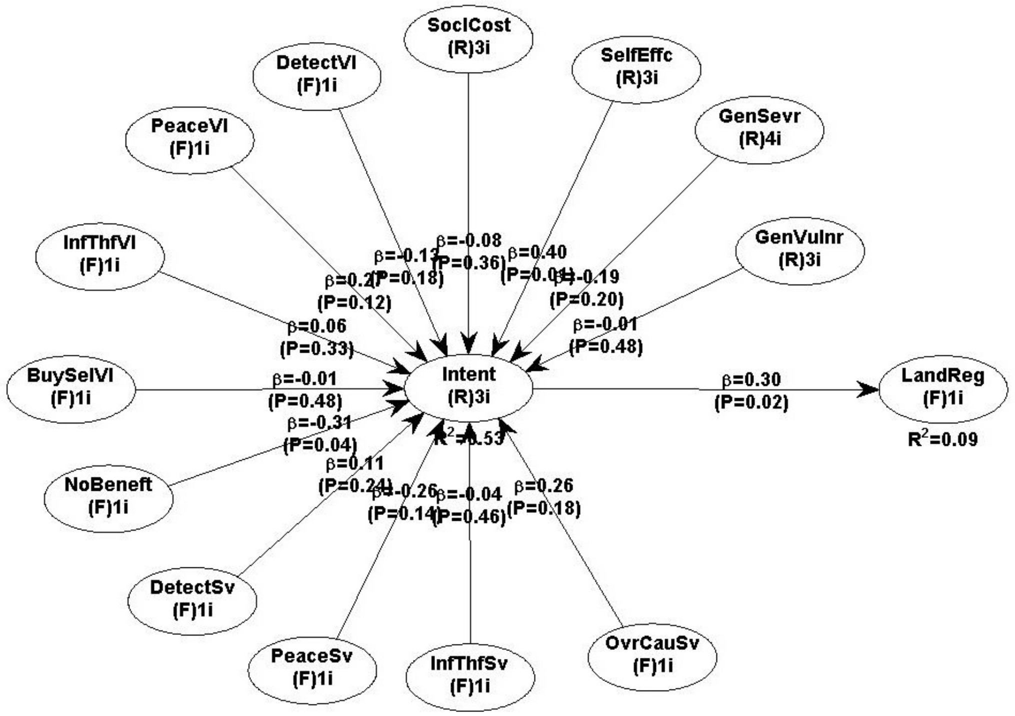
Credit Report



Variable	Description	Path Coefficient	P Value	Effect Size
Intent	Intention	**0.602**	**<0.001**	**0.362**
GenVulnr	General Vulnerability	0.027	0.433	0.005
GenSever	General Severity	-0.053	0.368	0.009
SelfEffc	Self-efficacy	0.172	0.167	0.045
SoclCost	Social Cost	-0.019	0.456	0.002
HisCorVl	History Correction Vulnerability	0.002	0.495	0.000
DetectVl	Detection Vulnerability	0.031	0.419	0.002
SecSnsVl	Secure Sense Vulnerability	-0.196	0.125	0.012
InfStlVl	Information Stolen Vulnerability	-0.016	0.445	0.002
HisCorSv	History Correction Severity	0.110	0.201	0.037
DetectSv	Detection Severity	0.210	0.068	0.088
SecSnsSv	Secure Sense Severity	0.110	0.259	0.043
InfStlSv	Information Stolen Severity	**0.292**	**0.010**	**0.057**
NoBeneft	No Benefit	**-0.303**	**0.008**	**0.113**
	Behaviour R Squared	0.362		
	Intention R Squared	0.370		

Bold indicates a P value less than 0.05

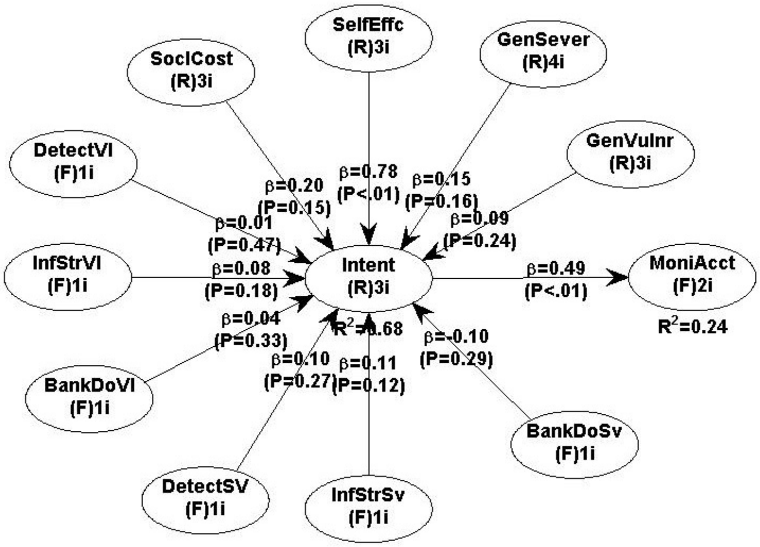
Land Registry



		Path	P	Effect
Variable	Description	Coefficient	Value	Size
Intent	Intention	**0.296**	**0.021**	**0.088**
GenVulnr	General Vulnerability	-0.015	0.480	0.003
GenSever	General Severity	-0.186	0.203	0.028
SelfEffc	Self-efficacy	**0.399**	**0.011**	**0.230**
SoclCost	Social Cost	-0.081	0.364	0.020
DetectVl	Detection Vulnerability	-0.129	0.184	0.028
PeaceVl	Peace of Mind Vulnerability	0.269	0.115	0.105
InfThfVl	Information Stolen Vulnerability	0.065	0.332	0.013
BuySelVl	Only when buying or selling vulnerability	-0.007	0.484	0.002
NoBeneft	No benefit	**-0.305**	**0.043**	**0.148**
DetectSv	Detection Severity	0.114	0.243	0.025
PeaceSv	Peace of Mind Severity	-0.263	0.141	0.012
InfThfSv	Information Stolen Severity	-0.042	0.458	0.002
OvrCauSv	Overly cautious Severity	0.256	0.180	0.098
	Behaviour R Squared	0.088		
	Intention R Squared	0.533		

Bold indicates a P value less than 0.05

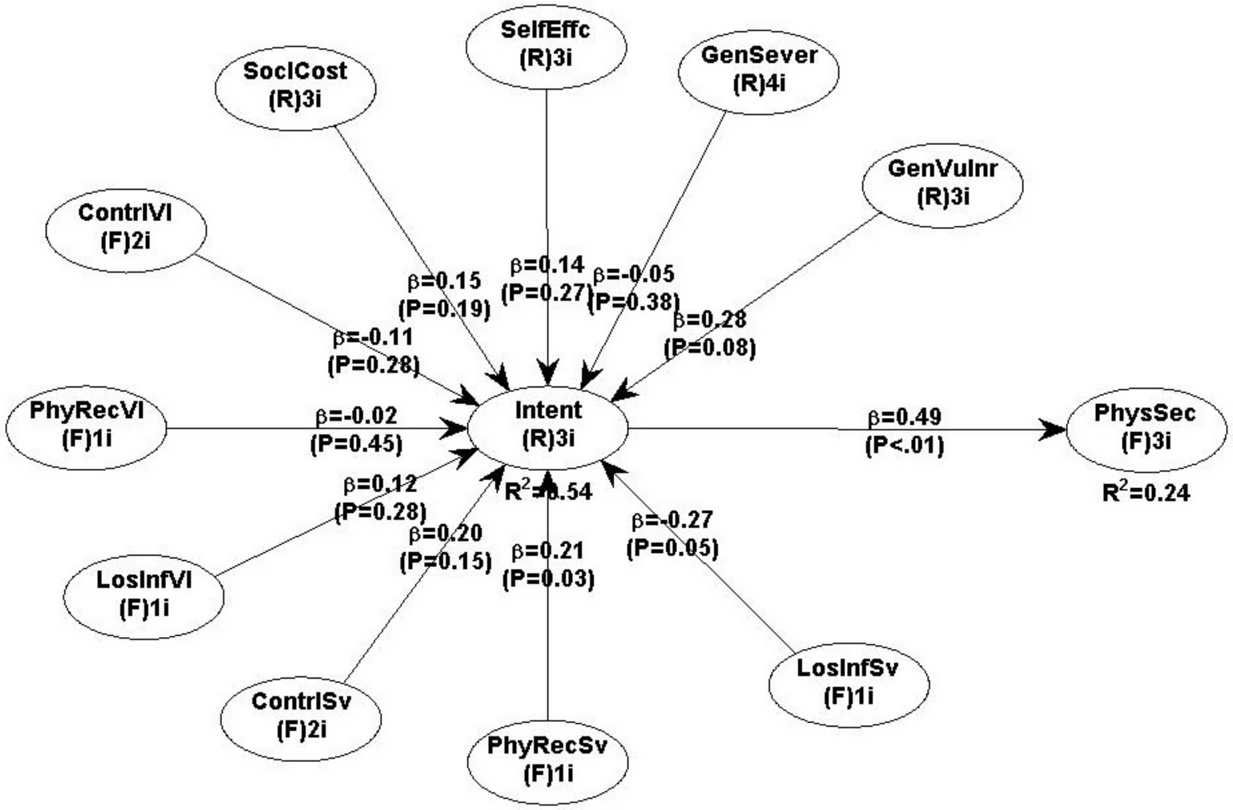
Monitoring Accounts



		Path	P	Effect
Variable	Description	Coefficient	Value	Size
Intent	Intention	**0.494**	**<0.001**	**0.244**
GenVulnr	General Vulnerability	0.091	0.244	0.028
GenSever	General Severity	0.149	0.161	0.058
SelfEffc	Self-efficacy	**0.775**	**<0.001**	**0.658**
SoclCost	Social Cost	0.199	0.146	0.130
DetectVl	Detect Unauthorized Use Vulnerability	0.005	0.475	0.002
InfStrVl	Info Stored on My Computer Vulnerability	0.078	0.183	0.025
BankDoVl	Bank Will Do It Vulnerability	0.036	0.334	0.009
DetectSv	Detect Unauthorized Use Severity	0.101	0.269	0.046
InfStrSv	Info Stored on My Computer Severity	0.107	0.116	0.026
BankDoSv	Bank Will Do It Severity	-0.103	0.287	0.034
	Behaviour R Squared	0.244		
	Intention R Squared	0.678		

Bold indicates a P value less than 0.05

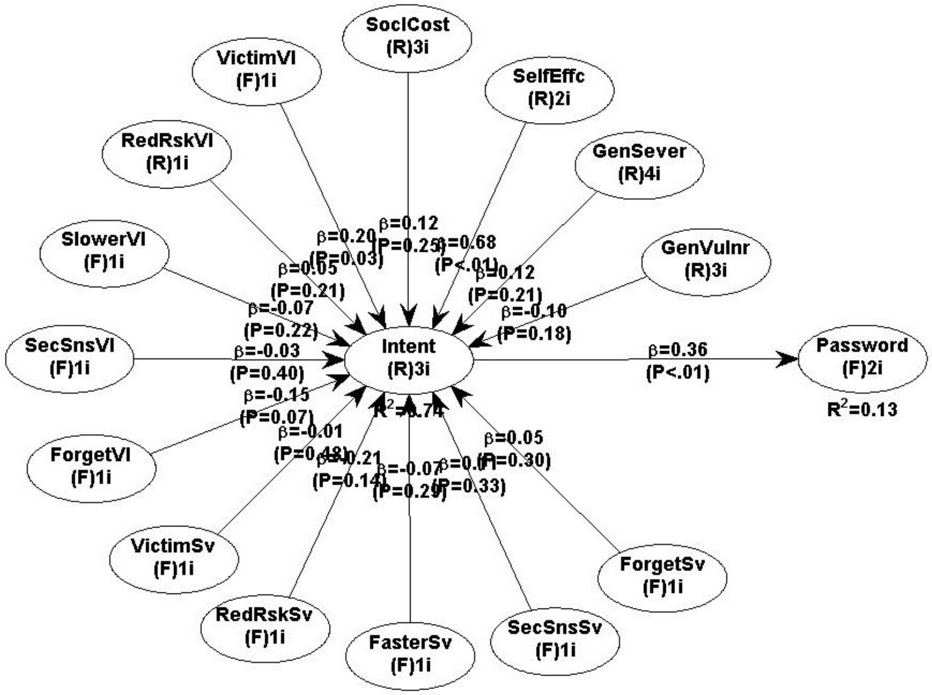
Physical Security



		Path	P	Effect
Variable	Description	Coefficient	Value	Size
Intent	Intention	**0.488**	**<0.001**	**0.238**
GenVulnr	General Vulnerability	0.277	0.085	0.141
GenSever	General Severity	-0.050	0.385	0.026
SelfEffc	Self-efficacy	0.142	0.270	0.071
SoclCost	Social Cost	0.152	0.186	0.088
ContrlVl	Control of Documents Vulnerability	-0.112	0.278	0.036
PhyRecVl	Have Physical Record Vulnerability	-0.017	0.448	0.006
LosInfVl	Lose Personal Identity Info Vulnerability	0.120	0.285	0.026
ContrlSv	Control of Documents Severity	0.204	0.148	0.111
PhyRecSv	Have Physical Record Severity	**0.207**	**0.033**	**0.092**
LosInfSv	Lose Personal Identity Info Severity	**-0.266**	**0.046**	**0.129**
	Behaviour R Squared	0.234		
	Intention R Squared	0.559		

Bold indicates a P value less than 0.05

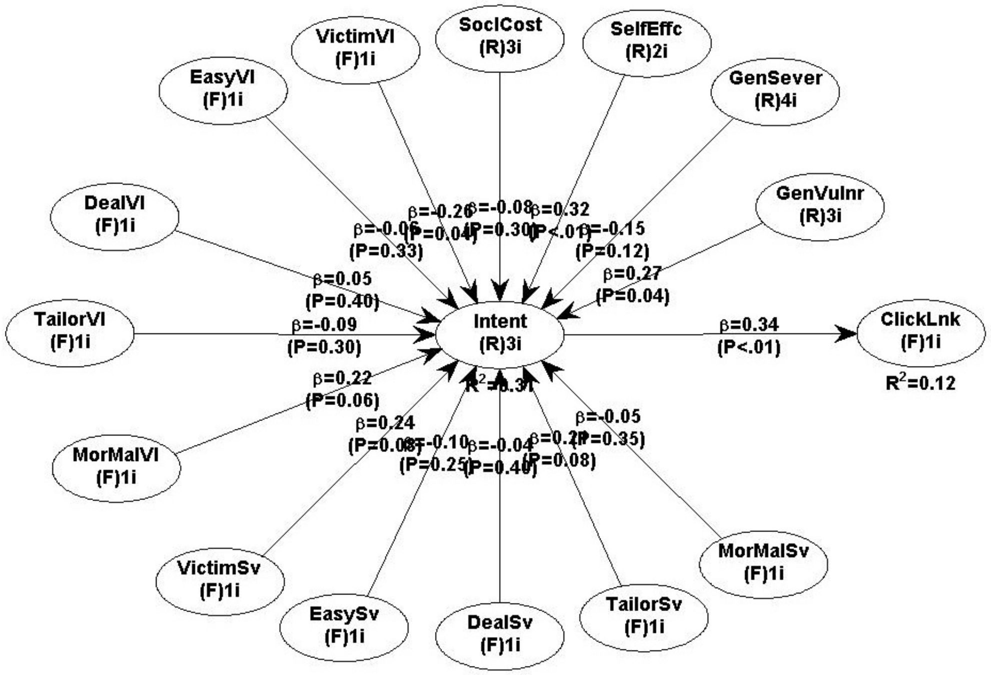
Password Security



Variable	Description	Path Coefficient	P Value	Effect Size
Intent	Intention	**0.359**	**<0.001**	**0.129**
GenVulnr	General Vulnerability	-0.102	0.184	0.034
GenSever	General Severity	0.117	0.213	0.060
SelfEffc	Self-efficacy	**0.679**	**<0.001**	**0.542**
SoclCost	Social Cost	0.121	0.246	0.067
VictimVl	Being Victimized Vulnerability	**0.204**	**0.034**	**0.074**
RedRskVl	Reducing Risk Vulnerability	0.050	0.214	0.016
SlowerVl	Online Access Speed Vulnerability	-0.075	0.221	0.023
SecSnsVl	Sense of Security Vulnerability	-0.035	0.398	0.015
ForgetVl	Forgetting Password Vulnerability	-0.155	0.074	0.066
VictimSv	Being Victimized Severity	-0.009	0.484	0.004
RedRskSv	Reducing Risk Severity	-0.208	0.145	0.097
FasterSv	Online Access Speed Severity	-0.066	0.286	0.011
SecSnsSv	Sense of Security Severity	0.115	0.335	0.056
ForgetSv	Forgetting Password Severity	0.052	0.296	0.008
	Behaviour R Squared	0.129		
	Intention R Squared	0.744		

Bold indicates a P value less than 0.05

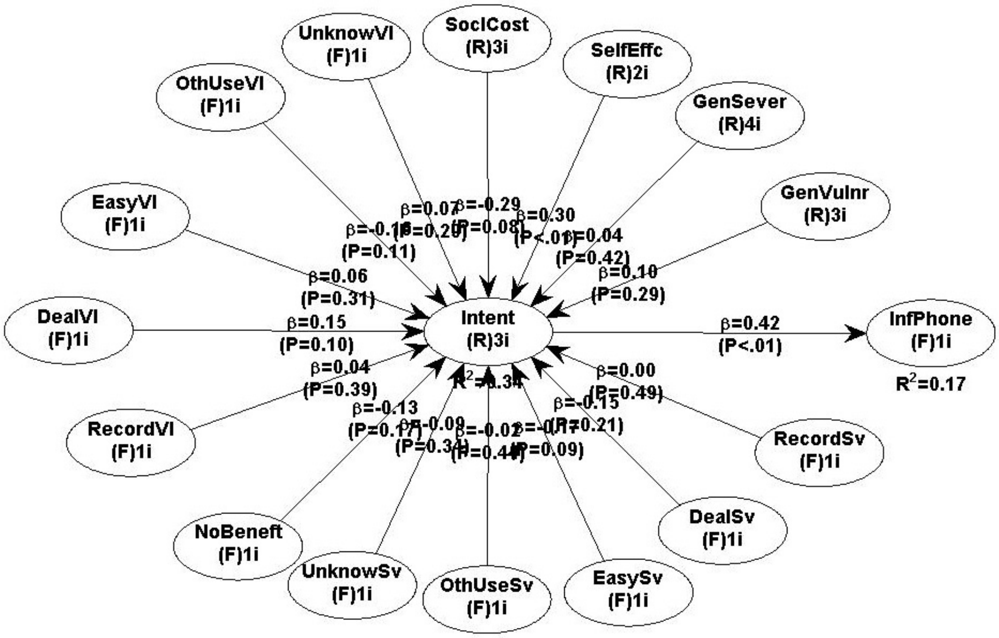
Click on Link in E-mail



Variable	Description	Path Coefficient	P Value	Effect Size
Intent	Intention	**0.340**	**0.003**	**0.116**
GenVulnr	General Vulnerability	**0.269**	**0.043**	**0.016**
GenSever	General Severity	-0.148	0.124	0.011
SelfEffc	Self-efficacy	**0.325**	**0.004**	**0.085**
SoclCost	Social Cost	-0.079	0.301	0.006
VictimVl	Malware Victim Vulnerability	**-0.263**	**0.043**	**0.053**
EasyVl	Easy and Convenient Vulnerability	-0.063	0.330	0.005
DealVl	Getting a Good Deal Vulnerability	0.049	0.398	0.008
TailorVl	Tailored Information Vulnerability	-0.094	0.301	0.003
MorMalVl	More E-mail Vulnerability	0.219	0.060	0.032
VictimSv	Malware Victim Severity	0.236	0.076	0.053
EasySv	Easy and Convenient Severity	-0.101	0.254	0.004
DealSv	Getting a Good Deal Severity	-0.041	0.405	0.003
TailorSv	Tailored Information Severity	0.210	0.076	0.032
MorMalSv	More E-mail Severity	-0.047	0.354	0.000
	Behaviour R Squared	0.116		
	Intention R Squared	0.306		

Bold indicates a P value less than 0.05

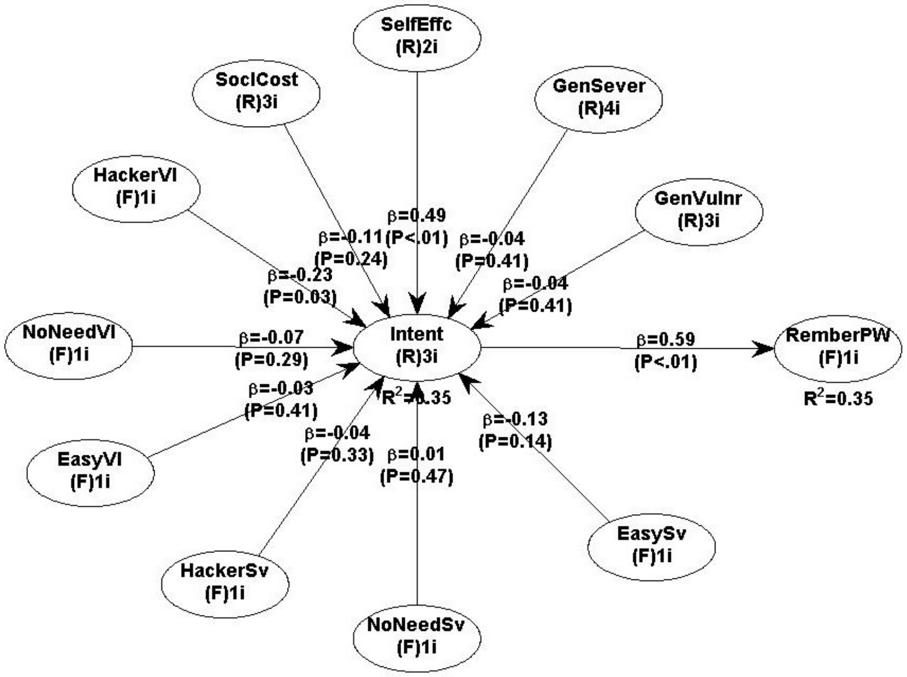
Give Personal Information Over the Phone



Variable	Description	Path Coefficient	P Value	Effect Size
Intent	Intention	**0.417**	**0.003**	**0.173**
GenVulnr	General Vulnerability	0.102	0.293	0.004
GenSever	General Severity	0.036	0.418	0.003
SelfEffc	Self-efficacy	**0.295**	**0.002**	**0.086**
SoclCost	Social Cost	-0.285	0.076	0.078
UnknowVl	Known Recipient Vulnerability	0.068	0.286	0.002
OthUseVl	Know How Info Used Vulnerability	-0.163	0.110	0.025
EasyVl	Convenience Vulnerability	0.056	0.311	0.003
DealVl	Saving Money Vulnerability	0.147	0.095	0.041
RecordVl	Having Transaction Record Vulnerability	0.039	0.385	0.006
NoBeneft	No Benefit Vulnerability	-0.129	0.169	0.020
UnknowSv	Known Recipient Severity	-0.086	0.336	0.023
OthUseSv	Know How Info Used Severity	-0.019	0.436	0.002
EasySv	Convenience Severity	-0.169	0.091	0.013
DealSv	Saving Money Severity	-0.153	0.212	0.048
RecordSv	Having Transaction Record Severity	0.004	0.490	0.001
	Intention R Squared	0.341		
	Behaviour R Squared	0.173		

Bold indicates a P value less than 0.05

Use 'Remember My Password'



		Path	P	Effect
Variable	Description	Coefficient	Value	Size
Intent	Intention	**0.593**	**<0.001**	**0.352**
GenVulnr	General Vulnerability	-0.040	0.409	0.009
GenSever	General Severity	-0.039	0.409	0.006
SelfEffc	Self-efficacy	**0.486**	**<0.001**	**0.241**
SoclCost	Social Cost	-0.108	0.237	0.023
HackerVl	Hackers Finding Password Vulnerability	**-0.225**	**0.031**	**0.068**
NoNeedVl	Not Having to Remember Password Vulnerability	-0.072	0.287	0.001
EasyVl	Making Web Sites Easy Vulnerability	-0.031	0.407	0.001
HackerSv	Hackers Finding Password Severity	-0.044	0.333	0.002
NoNeedSv	Not Having to Remember Password Severity	0.008	0.475	0.001
EasySv	Making Web Sites Easy Severity	-0.127	0.140	0.010
	Intention R squared	0.355		
	Behaviour R squared	0.352		

Bold indicates a P value less than 0.05

Appendix R – Phase 2 Qualitative Response Frequency Counts

In what ways do you think you are most vulnerable to identity theft?

Class	Code	#
Credit/Debit Card	Credit Card	55
	ATMs and PIN snooping	23
	Debit Card	12
	Unsolicited credit card applications	1
	Card skimming (incl. RFID and manual methods)	23
		114
Online	Online General	71
	Social Media	15
		86
Physical	Theft of documents - e.g. wallet, paper documents, credit card	48
	Snail Mail	16
	Social Insurance Number/Passports/Other Id documents	11
		75
Online Transactions	Online purchases/sales	58
	Online Banking	20
		78
Out of Personal Control	Data Breach	15
	Data collection by web sites/merchants/employers/government	19
	Being too trusting/Not protecting personal Information	27
		61
Personal Devices	Hackers/Malware	15
	Smart phones and other personal devices	4
	Unsecured wireless connections	2
	Info stored on computer (passwords, account numbers, etc.)	3
		24
Phishing	Phishing	7
	Surveys/contests (online, phone or mail)	6
	Phone general	17
		30
Passwords	Passwords	22
Not Vulnerable	Not vulnerable/My precautions are sufficient	9
Don't Know	Don't know/Everyone's vulnerable	33

Class	Code	#
Other	Travel	4
	New account fraud	3
	Existing Account Fraud	3
	Having a common/prominent name	3
	Age	1
	Lack of information	2
	Obstructive process for credit report	1
	No credit report	1
	Assets	2
		20

What do you think are the most important things you can do to prevent identity theft?

Class	Code	#
Credit/Debit Card	Guard PIN	52
	Minimize card use (use prepaid cards, cash, Paypal, etc.)	17
	Change PIN regularly	6
	Use RFID shield	1
	Report lost credit/debit cards	3
	Minimize number of bank accounts/credit cards	1
	Be aware when making transactions (machine or with person)	16
	Check for foreign hardware on bank machines	7
		103
Online	General internet carefulness	31
	Use secure web sites	40
	Avoid 'cloud' storage	1
	Limit info on social media sites	16
	Use pseudonyms online	3
	Privacy settings	2
		93
Physical	Shred/burn confidential documents	76
	Keep confidential documents in secure location	42
	Physical security - statements, credit cards, wallet, purse	18
	Minimize carried personal information	13
	Secure snail mail	4
	Don't divulge ID numbers (Social Insurance, passport, etc.)	13
		166
Online Transactions	Avoid on-line and/or mobile banking/transactions	11
	Avoid the internet-bank/shop in person	8
		19
Out of Personal Control	Deal with known entities (individuals/merchants/governments	47
	Notify financial institutions of planned travel activity	3
	Notify financial institution of unusual activity	7
		57
Personal Devices	Don't use auto fill (stored passwords etc.)	11
	Up to date security (anti-virus etc.) software	12
	Avoid public computers and WIFI	9
	Delete cookies/clear browsing history/sign out	9
	Don't store personal info on computer	2

Class	Code	#
		43
Phishing	General phone carefulness	49
	Don't click on suspect links or open suspect attachments	16
	Don't do surveys	5
	Don't fall for phishing (online or over phone)	15
	Avoid 'charities' online or on phone	1
		86
Passwords	Strong passwords	95
	Frequently change passwords	35
	Don't share or record passwords	30
	Multiple passwords	15
		175
General	General vigilance/Don't give out personal information	98
Doomed	Withdraw from the world	5
	Nothing! We're doomed!	2
		7
Don't Know	Don't Know	11
Other	Insurance (ID fraud, title, credit monitoring)	1
	Title insurance	2
	Hidden cameras	1
		4

What do you think are the most important things you can do to detect identity fraud?

Class	Code	#
Monitor Accounts	Monitor accounts	233
Check Credit Report	Check credit report	63
Check Property Registry	Check land registry	9
Use Service/Bank Will Do	Check for abnormalities on computer	2
	Use monitoring service/Bank will monitor	9
		11
'Google' Yourself	'Google' or otherwise investigate yourself	6
Nothing - We're Helpless	Nothing - we're helpless	3
Don't Know	Don't Know	42
Other	Set up alerts/anti-malware software notices	1
	Changed PIN	1
		2

Appendix S – Logistics Regression Analysis of Qualitative Data

1. In what ways do you think you are most vulnerable to identity theft?

Credit/Debit Cards

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-2.2783	0.4831	22.2355	<.0001		Intercept
N_ACCTS	1	0.0853	0.1052	0.6582	0.4172	1.089	# Bank Accounts
N_CARDS	1	0.1847	0.0973	3.6014	**0.0577**	1.203	# Credit Cards
AGE	1	0.00728	0.00833	0.7641	0.3820	1.007	Age
LANGUAGE	1	0.2265	0.2661	0.7246	0.3946	1.254	Language
SEX	1	-0.0252	0.2369	0.0113	0.9152	0.975	Gender
CARDVICT	1	0.2960	0.2561	1.3358	0.2478	1.345	Card Victim
OTHRVICT	1	0.2003	0.3591	0.3110	0.5771	1.222	Other Victim
OWNHOME	1	-0.0727	0.2488	0.0855	0.7700	0.930	Home Owner

Online

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-1.1977	0.5126	5.4588	0.0195		Intercept
N_ACCTS	1	0.0221	0.1158	0.0365	0.8484	1.022	# Bank Accounts
N_CARDS	1	-0.1741	0.1116	2.4318	0.1189	0.840	# Credit Cards
AGE	1	-0.00522	0.00910	0.3290	0.5662	0.995	Age
LANGUAGE	1	0.4904	0.2689	3.3257	**0.0682**	1.633	Language
SEX	1	0.3255	0.2574	1.5994	0.2060	1.385	Gender
CARDVICT	1	-0.2624	0.2979	0.7761	0.3784	0.769	Card Victim
OTHRVICT	1	0.0136	0.4079	0.0011	0.9734	1.014	Other Victim
OWNHOME	1	0.2614	0.2652	0.9720	0.3242	1.299	Home Owner

1. In what ways do you think you are most vulnerable to identity theft?

Online Transactions

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-0.5057	0.5230	0.9347	0.3336		Intercept
N_ACCTS	1	-0.0249	0.1236	0.0405	0.8405	0.975	# Bank Accounts
N_CARDS	1	0.0545	0.1153	0.2235	0.6364	1.056	# Credit Cards
AGE	**1**	**-0.0297**	**0.0102**	**8.3924**	**0.0038**	**0.971**	**Age**
LANGUAGE	**1**	**-1.4361**	**0.4021**	**12.7548**	**0.0004**	**0.238**	**Language**
SEX	**1**	**0.5880**	**0.2801**	**4.4081**	**0.0358**	**1.800**	**Gender**
CARDVICT	1	0.0477	0.2998	0.0253	0.8735	1.049	Card Victim
OTHRVICT	1	0.1797	0.4163	0.1864	0.6660	1.197	Other Victim
OWNHOME	1	0.0861	0.2845	0.0916	0.7622	1.090	Home Owner

Physical

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-2.3606	0.5465	18.6613	<.0001		Intercept
N_ACCTS	1	-0.00439	0.1233	0.0013	0.9716	0.996	# Bank Accounts
N_CARDS	1	-0.0192	0.1139	0.0283	0.8663	0.981	# Credit Cards
AGE	1	0.0154	0.00939	2.6799	0.1016	1.015	Age
LANGUAGE	1	-0.3454	0.3292	1.1007	0.2941	0.708	Language
SEX	1	0.1328	0.2722	0.2380	0.6256	1.142	Gender
CARDVICT	1	0.2829	0.2928	0.9332	0.3340	1.327	Card Victim
OTHRVICT	1	0.3227	0.3998	0.6514	0.4196	1.381	Other Victim
OWNHOME	1	0.00991	0.2847	0.0012	0.9722	1.010	Home Owner

1. In what ways do you think you are most vulnerable to identity theft?

Out of Personal Control

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-2.2083	0.5855	14.2265	0.0002		Intercept
N_ACCTS	1	0.1655	0.1354	1.4934	0.2217	1.180	# Bank Accounts
N_CARDS	**1**	**-0.3148**	**0.1336**	**5.5528**	**0.0185**	**0.730**	**# Credit Cards**
AGE	**1**	**0.0237**	**0.0101**	**5.5429**	**0.0186**	**1.024**	**Age**
LANGUAGE	1	0.3745	0.3234	1.3415	0.2468	1.454	Language
SEX	1	-0.4149	0.2935	1.9988	0.1574	0.660	Gender
CARDVICT	**1**	**0.6403**	**0.3175**	**4.0668**	**0.0437**	**1.897**	**Card Victim**
OTHRVICT	1	0.0668	0.4457	0.0225	0.8808	1.069	Other Victim
OWNHOME	**1**	**-0.7499**	**0.3047**	**6.0567**	**0.0139**	**0.472**	**Home Owner**

2. What do you think are the most important things you can do to prevent identity theft?

Credit/Debit Cards

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-2.2211	0.5024	19.5471	<.0001		Intercept
N_ACCTS	1	-0.0863	0.1136	0.5769	0.4475	0.917	# Bank Accounts
N_CARDS	1	0.0542	0.1029	0.2776	0.5983	1.056	# Credit Cards
AGE	**1**	**0.0172**	**0.00858**	**4.0010**	**0.0455**	**1.017**	**Age**
LANGUAGE	1	0.2627	0.2737	0.9213	0.3371	1.300	Language
SEX	1	0.1976	0.2484	0.6329	0.4263	1.218	Gender
CARDVICT	1	0.1128	0.2726	0.1714	0.6789	1.119	Card Victim
OTHRVICT	1	0.3663	0.3661	1.0014	0.3170	1.442	Other Victim
OWNHOME	1	-0.0689	0.2571	0.0718	0.7887	0.933	Home Owner

Online

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-1.7745	0.5040	12.3981	0.0004		Intercept
N_ACCTS	1	0.0654	0.1126	0.3379	0.5610	1.068	# Bank Accounts
N_CARDS	1	0.0856	0.1059	0.6543	0.4186	1.089	# Credit Cards
AGE	1	-0.00922	0.00898	1.0535	0.3047	0.991	Age
LANGUAGE	1	0.0995	0.2805	0.1259	0.7227	1.105	Language
SEX	**1**	**0.6773**	**0.2607**	**6.7519**	**0.0094**	**1.969**	**Gender**
CARDVICT	1	0.4469	0.2702	2.7347	**0.0982**	1.563	Card Victim
OTHRVICT	1	0.0226	0.3839	0.0035	0.9531	1.023	Other Victim
OWNHOME	1	-0.2085	0.2596	0.6451	0.4219	0.812	Home Owner

2. What do you think are the most important things you can do to prevent identity theft?

Physical

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-1.6553	0.4372	14.3337	0.0002		Intercept
N_ACCTS	1	-0.0964	0.0992	0.9437	0.3313	0.908	# Bank Accounts
N_CARDS	1	0.1575	0.0904	3.0387	**0.0813**	1.171	# Credit Cards
AGE	**1**	**0.0151**	**0.00757**	**3.9776**	**0.0461**	**1.015**	**Age**
LANGUAGE	1	-0.1352	0.2492	0.2946	0.5873	0.874	Language
SEX	1	0.2447	0.2175	1.2658	0.2605	1.277	Gender
CARDVICT	1	0.0152	0.2409	0.0040	0.9497	1.015	Card Victim
OTHRVICT	1	-0.2921	0.3594	0.6602	0.4165	0.747	Other Victim
OWNHOME	1	0.0468	0.2268	0.0425	0.8367	1.048	Home Owner

Out of Personal Control

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-2.5781	0.6116	17.7713	<.0001		Intercept
N_ACCTS	1	0.0983	0.1339	0.5388	0.4629	1.103	# Bank Accounts
N_CARDS	1	-0.0976	0.1287	0.5750	0.4483	0.907	# Credit Cards
AGE	1	0.00956	0.0104	0.8528	0.3558	1.010	Age
LANGUAGE	1	-0.2433	0.3547	0.4705	0.4928	0.784	Language
SEX	1	0.4786	0.3072	2.4262	0.1193	1.614	Gender
CARDVICT	1	0.0801	0.3319	0.0582	0.8094	1.083	Card Victim
OTHRVICT	1	-0.2894	0.5099	0.3220	0.5704	0.749	Other Victim
OWNHOME	1	0.1033	0.3138	0.1083	0.7421	1.109	Home Owner

2. What do you think are the most important things you can do to prevent identity theft?

Phishing

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-2.5885	0.5345	23.4526	<.0001		Intercept
N_ACCTS	1	-0.0750	0.1220	0.3784	0.5385	0.928	# Bank Accounts
N_CARDS	1	0.0416	0.1106	0.1419	0.7064	1.043	# Credit Cards
AGE	**1**	**0.0313**	**0.00911**	**11.7890**	**0.0006**	**1.032**	**Age**
LANGUAGE	1	-0.5808	0.3367	2.9751	**0.0846**	0.559	Language
SEX	1	0.2261	0.2668	0.7182	0.3968	1.254	Gender
CARDVICT	1	-0.2713	0.3049	0.7922	0.3734	0.762	Card Victim
OTHRVICT	1	0.2260	0.4035	0.3138	0.5754	1.254	Other Victim
OWNHOME	1	-0.3364	0.2757	1.4893	0.2223	0.714	Home Owner

Passwords

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	0.2189	0.4195	0.2723	0.6018		Intercept
N_ACCTS	1	0.1062	0.0958	1.2285	0.2677	1.112	# Bank Accounts
N_CARDS	1	0.00372	0.0901	0.0017	0.9671	1.004	# Credit Cards
AGE	**1**	**-0.0222**	**0.00774**	**8.2547**	**0.0041**	**0.978**	**Age**
LANGUAGE	1	-0.4781	0.2475	3.7321	**0.0534**	0.620	Language
SEX	1	0.1789	0.2132	0.7045	0.4013	1.196	Gender
CARDVICT	1	-0.3243	0.2426	1.7866	0.1813	0.723	Card Victim
OTHRVICT	1	-0.1417	0.3447	0.1690	0.6810	0.868	Other Victim
OWNHOME	1	0.0689	0.2221	0.0961	0.7566	1.071	Home Owner

2. What do you think are the most important things you can do to prevent identity theft?

General Caution

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-0.4237	0.4705	0.8110	0.3678		Intercept
N_ACCTS	1	0.0330	0.1089	0.0919	0.7618	1.034	# Bank Accounts
N_CARDS	1	-0.1917	0.1042	3.3830	**0.0659**	0.826	# Credit Cards
AGE	1	-0.00326	0.00846	0.1480	0.7005	0.997	Age
LANGUAGE	1	0.1093	0.2633	0.1721	0.6782	1.115	Language
SEX	1	-0.2324	0.2373	0.9591	0.3274	0.793	Gender
CARDVICT	1	-0.4985	0.2867	3.0245	**0.0820**	0.607	Card Victim
OTHRVICT	1	-0.0286	0.3898	0.0054	0.9415	0.972	Other Victim
OWNHOME	1	0.0467	0.2471	0.0357	0.8502	1.048	Home Owner

3. What do you think are the most important things you can do to detect identity fraud?

Monitor Accounts

Analysis of Maximum Likelihood Estimates							
Parameter	DF	Estimate	Standard Error	Chi-Square	Pr > ChiSq	Odds Ratio	Label
Intercept	1	-0.1140	0.4132	0.0762	0.7826		Intercept
N_ACCTS	1	0.1010	0.0955	1.1174	0.2905	1.106	# Bank Accounts
N_CARDS	1	0.0904	0.0883	1.0494	0.3057	1.095	# Credit Cards
AGE	1	-0.00795	0.00737	1.1635	0.2807	0.992	Age
LANGUAGE	**1**	**-0.6825**	**0.2343**	**8.4880**	**0.0036**	**0.505**	**Language**
SEX	**1**	**0.6051**	**0.2091**	**8.3753**	**0.0038**	**1.832**	**Gender**
CARDVICT	1	0.3307	0.2362	1.9606	0.1615	1.392	Card Victim
OTHRVICT	1	0.2959	0.3414	0.7511	0.3861	1.344	Other Victim
OWNHOME	1	0.00912	0.2172	0.0018	0.9665	1.009	Home Owner

Check Credit Report

Analysis of Maximum Likelihood Estimates							
Parameter	DF	Estimate	Standard Error	Chi-Square	Pr > ChiSq	Odds Ratio	Label
Intercept	1	-1.6185	0.5463	8.7777	0.0030		Intercept
N_ACCTS	1	0.2391	0.1266	3.5653	**0.0590**	1.270	# Bank Accounts
N_CARDS	1	-0.0286	0.1222	0.0546	0.8152	0.972	# Credit Cards
AGE	1	-0.00787	0.0101	0.6053	0.4366	0.992	Age
LANGUAGE	**1**	**-1.6621**	**0.4873**	**11.6320**	**0.0006**	**0.190**	**Language**
SEX	1	0.2280	0.2893	0.6213	0.4306	1.256	Gender
CARDVICT	1	-0.0333	0.3191	0.0109	0.9168	0.967	Card Victim
OTHRVICT	1	0.6033	0.4001	2.2741	0.1316	1.828	Other Victim
OWNHOME	1	-0.3299	0.2998	1.2110	0.2711	0.719	Home Owner

3. What do you think are the most important things you can do to detect identity fraud?

Don't Know

Analysis of Maximum Likelihood Estimates							
Parameter	**DF**	**Estimate**	**Standard Error**	**Chi-Square**	**Pr > ChiSq**	**Odds Ratio**	**Label**
Intercept	1	-1.3167	0.6916	3.6243	0.0569		Intercept
N_ACCTS	1	-0.1453	0.1626	0.7976	0.3718	0.865	# Bank Accounts
N_CARDS	1	-0.1268	0.1465	0.7487	0.3869	0.881	# Credit Cards
AGE	1	-0.0156	0.0129	1.4720	0.2250	0.984	Age
LANGUAGE	**1**	**0.6931**	**0.3495**	**3.9332**	**0.0473**	**2.000**	**Language**
SEX	1	-0.4804	0.3384	2.0160	0.1556	0.619	Gender
CARDVICT	**1**	**0.7730**	**0.3555**	**4.7286**	**0.0297**	**2.166**	**Card Victim**
OTHRVICT	1	-0.9678	0.7571	1.6341	0.2011	0.380	Other Victim
OWNHOME	1	0.4536	0.3633	1.5589	0.2118	1.574	Home Owner

Appendix T – MANOVA of Random Selection

Demographic Variables

Variable	Type III Sum of Squares	df	Mean Square	F	Sig.
Number Bank Accounts	7.220	4	1.805	1.328	.259
Number Credit Cards	14.403	4	3.601	2.184	.070
Age	363.067	4	90.767	.441	.779
Language	1.206	4	.301	1.614	.170
Gender	.315	4	.079	.316	.868
Home Owner	.461	4	.115	.487	.745

Post Hoc Test - Tukey's HSD - Number of Credit Cards

(I) Random Section Selection	(J) Random Section Selection	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
Credit Report	Monitoring	-.39	.213	.351	-.98	.19
	Password	.04	.214	1.000	-.55	.63
	Physical	.19	.213	.906	-.40	.77
	Risky	-.23	.204	.796	-.79	.33
Monitoring	Credit Report	.39	.213	.351	-.19	.98
	Password	.43	.224	.302	-.18	1.05
	Physical	.58	.223	.072	-.03	1.19
	Risky	.16	.215	.940	-.42	.75
Password	Credit Report	-.04	.214	1.000	-.63	.55
	Monitoring	-.43	.224	.302	-1.05	.18
	Physical	.15	.224	.966	-.47	.76
	Risky	-.27	.216	.723	-.86	.32
Physical	Credit Report	-.19	.213	.906	-.77	.40
	Monitoring	-.58	.223	.072	-1.19	.03
	Password	-.15	.224	.966	-.76	.47
	Risky	-.42	.214	.298	-1.00	.17
Risky	Credit Report	.23	.204	.796	-.33	.79
	Monitoring	-.16	.215	.940	-.75	.42
	Password	.27	.216	.723	-.32	.86
	Physical	.42	.214	.298	-.17	1.00