2010 Second Cybercrime and Trustworthy Computing Workshop

Understanding Victims of Identity Theft: Preliminary Insights

Kylie Turville
Internet Commerce
Security Laboratory
University of Ballarat
Email: k.turville@ballarat.edu.au

John Yearwood
Center for Informatics and
Applied Optimization
University of Ballarat
Email: j.yearwood@ballarat.edu.au

Charlynn Miller
Center for Informatics and
Applied Optimization
University of Ballarat
Email: c.miller@ballarat.edu.au

***Abstract*—Identity theft is not a new crime, however changes in society and the way that business is conducted have made it an easier, attractive and more lucrative crime. When a victim discovers the misuse of their identity they must then begin the process of recovery, including fixing any issues that may have been created by the misuse. For some victims this may only take a small amount of time and effort, however for others they may continue to experience issues for many years after the initial moment of discovery. To date, little research has been conducted within Australia or internationally regarding what a victim experiences as they work through the recovery process. This paper presents a summary of the identity theft domain with an emphasis on research conducted within Australia, and identifies a number of issues regarding research in this area. The paper also provides an overview of the research project currently being undertaken by the authors in obtaining an understanding of what victims of identity theft experience during the recovery process; particularly their experiences when dealing with organizations. Finally, it reports on some of the preliminary work that has already been conducted for the research project.**

I. Introduction

An identity is valuable [26]. To the individual, their identity provides them with a sense of self, and a way of distinguishing themselves from all others. Within society, an individual's identity provides them with the ability to participate and to verify their identity to others, particularly in light of relatively recent changes such as a more transient population, technological advances, globalization, a move away form face-to-face transactions, and a move towards a cashless society.

Criminals have long known the value of being able to use or adopt another identity. Being able to remain anonymous or to use another individual's identity provides the criminal with the ability to commit fraud and other crimes without the crimes being associated with their own identity. Alternatively, when an individual's own identity is not able to be used effectively due to criminal records, bad credit ratings, or a lack of credentials, being able to adopt or use the identity of another individual is one way of circumventing these issues.

Once a victim of identity theft discovers the misuse, they then need to start working through any issues that may have been created [32]. Studies indicate that for a large proportion of victims this may only take a phone call and a small number of hours. However, a small number of victims find that they are having to deal with the problems created for many years after the discovery of the misuse [21].

In order for a victim to be considered recovered they need to be able to return to the same, if not better, state that they enjoyed prior to the victimization [15]. Victims of crime may generally be impacted three different ways: financially, physically, and/or emotionally. Depending on how the victim has been impacted there may be number of different areas that a victim needs to address whilst working towards recovery. Evidence from the research that has been conducted indicates that there are some victims that are not able to achieve this state of recovery.

Internationally a relatively large amount of predominantly qualitative research has been conducted pertaining to identity theft victims, particularly within the United States. The Identity Theft Resource Center (ITRC) [21] and Javelin Strategy and Research [24] are responsible for the majority of the research conducted in the identity theft domain focusing on victims; other studies have been conducted by the Center for Identity Management and Information Protection (CIMIP) [11], and the California Public Interest Research Group (CALPIRG) [7]. Within Australia, there have only been a very limited number of studies conducted within this area, with the main studies having been completed by the Australian Bureau of Statistics (ABS) [6], the Office of the Privacy commissioner (OPC) [42], and Galaxy Research [17].

In terms of the research that has been conducted, there is still not much known about victims and how they deal with the resulting issues created by the theft of their identity. This research is investigating the interaction between the organizations involved and the victim, and as such, will predominantly focus on the financial impact upon the victim, with some information regarding the emotional impact being obtained.

II. The Research

The focus of this research is on developing an understanding of what a victim of identity theft experiences from the moment that they discover that their identity has been misused. The research aims to provide a thorough understanding of how a victim of identity theft works through the recovery of their identity, what processes organizations currently use to assist victims, what impact the processes used by organizations have

978-0-7695-4186-0/10 $26.00 © 2010 IEEE
DOI 10.1109/CTC.2010.12

upon the victim, the effectiveness of the processes and what opportunities exist for improvement.

In this paper, we provide an overview of the current literature focusing on identity theft (section III), studies conducted relating to victims of identity theft (section IV), and the concept of victim recovery(sections V). We also highlight the grounded theory methodology that will be utilized for this research project, including the details of the data that will be collected. (section VII). Finally we present some preliminary results (section VIII).

III. An Overview of Identity Theft

One of the main issues faced by researchers within this domain is the lack of consistency with regards to terminology. The three main terms used within the literature are identity theft, identity fraud and identity crime. In many instances, the terms identity theft and identity fraud are used interchangeably. There have been a number of attempts made by researchers to provide standardized definitions for the terminology, but none have been adopted sufficiently for them to be considered definitive [4], [22], [12], [40].

For this work the definitions provided by the Australasian Center for Policing Research (ACPR) [4] are used. These definitions are inclusive, and have been developed with a focus on individuals as well as the Australian identification system. The definitions provided by the ACPR are:

- identity theft: "the theft or assumption of a pre-existing identity (or significant part thereof), with or without consent, and, whether, in the case of an individual, the person is living or deceased";
- identity fraud: "the gaining of money, goods, services other benefits or the avoidance of obligations through the use of a fabricated identity; a manipulated identity; or a stolen/assumed identity"; and
- identity crime: "a generic term to describe activities/offences in which a perpetrator uses a fabricated identity; a manipulated identity; or a stolen/assumed identity to facilitate the commission of a crime(s)".

For the definitions provided by the ACPR, a fabricated identity is one that is not based on any other identity and is entirely fictitious; whereas a manipulated identity is an already existing identity that has been altered to create a new identity.

Most identity theft incidents involve the victim's identity being used by the perpetrator to commit fraud. Historically the organization against whom the fraud was perpetrated was the legally recognized victim of the crime leaving the individual whose identity had been misused with very little recourse for justice or recovery. It is now accepted that there are often two victims of this one crime - the primary victim being the organization and the secondary victim being the individual (or business) whose identity has been misused. Changes in the legislation of a number of Australian states have been introduced to legally recognize the individual as an official victim of crimes.

McNally and Newman have identified three stages of identity theft (see Figure:1), the acquisition of the information or documentation required (Time 1), the misuse of the identity (Time 2), and the outcomes of the misuse (Time 3) [30].

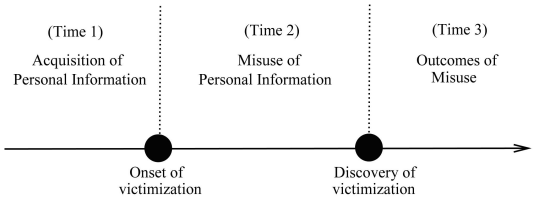

Fig. 1. Three stages of identity theft from [30]

During Time 1 (acquisition) the perpetrator obtains the information and/or documentation that they require in order to use the identity of the victim. The requirements are often dependent on how the perpetrator intends to use the identity. The perpetrator may use technology-enabled methods or the traditional methods of obtaining this information; including phishing, dumpster-diving, stealing wallets or documents, credit-card skimming and obtaining forgeries of documents [32], [31], [29]. If forgeries are used, the perpetrator may also take advantage of the circular nature of identification, particularly within Australia, and use the forgeries to obtain legitimate documents. Many perpetrators utilize the "weak-links" within the system in order to build up an identity [23].

Once the perpetrator has what they require, they then move into Time 2 (misuse); as this second time period begins, the onset of victimization occurs. The perpetrator uses the identity to perpetrate a fraudulent activity; this may involve accessing new lines of credit, committing employment and/or tax fraud, money laundering, drug trafficking, opening of utilities accounts, obtaining accommodation, and illegal immigration [22], [12], [40], [32]. Further to this, if the perpetrator uses identity whilst committing a criminal offence, this may result in a criminal record being created in the victim's name [32], [7].

Time 3 (outcomes) begins when the victim becomes aware of the misuse of their identity; this may happen within a matter of hours or the victim may not become aware of any issues until years later. The victim can discover the misuse in a number of ways including having new applications for lines of credit rejected, being sent bills for services or utilities that they have not used, visits by debt collectors, being contacted by their financial institution regarding suspicious activity on their account or even by being arrested for a crime that they did not commit [21], [32]. Once the misuse is discovered, the victim must then start to work through the issues that may have been created. As previously mentioned, research indicates that for some victims this task may only take a phone call and a small number of hours, however for a small number of victims this may be the start of an arduous task that may take many years to resolve [21].

Little is known about the specifics regarding what a victim experiences during Time 3 [22], [30]. Although a number of studies have been conducted regarding victims of identity theft,

they are mostly quantitative in nature and do not provide an in-depth understanding of the experiences. An understanding of the obstacles and issues that a victim faces during the process of recovering from the incident(s) is required in order to be able to improve the current processes that are used.

IV. Victims of Identity Theft Research

A number of studies relating to identity theft victims have been conducted in Australia and also internationally. The first known study that focused on victims was conducted in 1996 by the California Public Interest Research Group (CALPIRG) [32]. The majority of these studies have been undertaken in the United States where the key piece of information used by perpetrators of identity theft is an individual's Social Security Number (SSN) [8]; compared with Australia where there is no key piece of information that is capable of identifying an individual.

The following section provides a summary of some of the main studies completed with a focus on those who have looked at the victims experience after the discovery of the misuse.

A. International Studies

The California Public Interest Research Group (CALPIRG) conducted the first known study on identity theft in 1996, followed by another in 1997 [7]. The study was small in size (n=56) and only included individuals who had made a complaint to CALPIRG, thus limiting the generalizability of the study. The study found that victims faced many obstacles whilst trying to resolve the issues related to the theft of their identity. Less than half of the participants of the study felt that they had been able to fully resolve all of the issues relating to the theft of their identity, and those with unresolved cases had been dealing with the issues for an average of four years. The victims had spent a mean of 175 hours and $US808 in costs to deal with the issues. One of the main difficulties faced by victims was dealing with the different organizations involved, including law enforcement agencies. Many reported that the organizations were unhelpful and very difficult to deal with.

The Identity Theft Resource Center, established in the United States in 1999 (originally named VOICES), has conducted six studies relating to victims of identity theft and the impact of the crime on the victim [21]. The study contains comparisons with five other studies conducted since 2005. The study is limited in its generalizability as the survey is only sent to individuals who reported an incident of identity theft to the ITRC during 2008. The study found that victims spend on average 58 hours repairing the damage done to an already existing account and over 165 hours to fix problems created by the perpetrator opening new accounts in their name. The participants also reported that a number of the issues that they faced when trying to clear records and fix the problems associated with the misuse were "beyond their control", and that in some cases the victims had given up.

An exploratory study of identity theft victims conducted by Sharp et al. [36] focused on the psychological and somatic impact of the incident on the victim. Due to the small number of participants the generalizability of the study is limited (n=37). The study was conducted in three parts, these being a victim impact questionnaire, a Brief Symptom Inventory-18 (BSI-18) and a focus group. The BSI-18 is a standard test used to measure psychological distress and psychiatric disorders [33].

The victim impact questionnaire used open-ended questions to investigate the psychological effects on the victim after learning about the identity theft [36]. The questions focused on two time periods, these being two weeks and then twenty six weeks, after the discovery. Initially the most common reactions were feelings of irritation and anger, along with anxiety and fear. However at twenty six weeks, the victim's emotional response altered and feelings of distress, desperation, irritation and anger were being experienced. The main physical response at two weeks related to sleep issues, however this altered at the 26 week mark, with the main physical response being anxiety and nervousness. The results of the BSI-18 tests (n=30) indicate that those individuals who still had unresolved issues relating to the theft of their identity had higher means on all of the subscales, and those relating to somatization and depression were found to be statistically significant [36].

The latest study was conducted by Javelin Strategy and Research. Javelin reports that identity fraud is on the increase, with more victims in the last year than in any other period since they began their work in 2003 [24]. The main increase was in the area of new accounts fraud, where the victim's identity has been used to open new accounts and obtain new lines of credit. New accounts fraud is generally more difficult for the victim to detect, and is often associated with longer time periods and money to resolve the issues [21], [32].

B. Australian Studies

Only a limited amount of research has been conducted regarding identity theft victims within Australia. Many of the studies have only included identity theft as a small part of a much larger study and have only obtained small amounts of quantitative information.

The Australian Bureau of Statistics (ABS) included a section on identity theft in their Personal Fraud survey conducted in 2007 [6]. The survey was qualitative in nature and focused on the demographics of the victims, the method of fraud, whether the victim had reported the incident, who the victim reported the incident to, the amount of time and money lost and whether they had changed their behavior as a result of the incident. The definitions used by the ABS may have had a limiting effect on the study; these being:

- identity fraud: "comprises bank or credit card fraud"
- identity theft: "includes the fraudulent use of personal details such as a drivers license or tax file number, without permission, or illegally appropriating another person's identity for unauthorized gain."

The study found that 12.8% of victims spent more than 20 hours resolving the issues and that 19.8% felt that the issue had not yet been fully resolved. No data was collected regarding how the victims spent this time.

The Office of the Privacy Commissioner (OPC) included a small number of questions regarding identity theft in their study of "Community Attitudes to Privacy 2007" [42]. The main aim the questions regarding identity theft was to determine the participants' attitudes towards privacy and identity, and details were collected regarding how victims dealt with the outcomes. Identity theft was described to the participants as "an individual obtains your personal information such as credit card, driver's license, passport or other personal identification documents and uses these to obtain a benefit or service for themselves fraudulently"; this definition is relatively restrictive as it only includes tokens of identity. Only a very small amount of time was spent on the section pertaining to identity theft; according to their documentation on average only two minutes was spent on the questions in this section [42].

The most recent Australian study was conducted by Galaxy Research for Veda Advantage [13]. The main aim of this study was to determine if participants had taken steps to protect themselves from identity theft, such as using the service which is available to inform the individual that someone has used their details to apply for credit. Very little detail was made available, the survey was very short, did not obtain any in-depth information and did not collect any information regarding the experiences of victims.

None of the studies above used a previously defined definition for identity theft or identity fraud [4], [22], [40], rather they developed their own distinct definitions, thus making comparisons among the studies difficult. None of the studies obtained in-depth information regarding the experiences of the victims.

C. Summary

The majority of work relating to victims of identity theft has been conducted internationally. Due to the differences in the identification systems, cultures, legislation and legal systems of the different countries it is not possible to directly extend these results to the population of Australia. However they can still be used as a guide in regards to problems that victims may face. The studies indicate that victims face a number of issues, particularly in relation to working with organizations. Victims experience problems when trying to clear or remove any records that may have been created, retrieving money removed from their accounts, and generally trying to resolve any issues that have been created.

V. Victim Recovery and Identity Theft

Victim recovery is one of the key concepts of victimology and occurs when the victim is provided with the assistance and support that they require to return to the same, if not better, state that they experienced prior to the crime being committed [16].

Generally victims of crime may be impacted in three different ways: financially, physically and/or emotionally. Each victim will react in a different way and their reactions may be dependent upon the type of crime, their relationship with the offender, as well as their emotional state prior to being victimized. The work conducted by Sharp et al. [36] indicates that the longer the victim experiences difficulties, the more intense the physical and psychological problems.

Victims of identity theft are not often physically present during the act, and as such may not experience a direct physical impact. Research indicates that victims may experience indirect physical impacts as a result of the trauma, especially in cases where the issues created by the misuse take a long time to resolve [36], [37].

Financially the victim may either be directly or indirectly impacted by the crime. Directly the victim may lose money from their accounts or be identified as the person responsible for a debt. Indirectly, they may be financially impacted due to a loss of income, medical or legal expenses, loss of employment, moving costs, higher insurance premiums, and other costs [21].

The emotional impact can be experienced in the short, medium or long term. The victim may experience shock, confusion, helplessness, depression, panic symptoms, grief, confusion, trust issues, and even develop anxiety disorders such as agoraphobia or obsessive-compulsive disorder. Emotionally the response may be so severe that the victim may develop some form of psychiatric problem, for example a Posttraumatic Stress Disorder [19]. The emotional, or psychological, impact experienced may depend upon a number of issues including the offender/victim relationship, the perception that the victim has of the legal system, the treatment that they obtain, issues relating to compensation, the nature of the crime, and the victims state prior to the offense [16].

Victims of personal violence crimes are generally viewed as having been impacted more severely than victims of non-violent crime, for example white-collar crime, however this is not always the case. Shover [37] found that the effects of white-collar crime can "echo" that of violent crime, and that the effects can be felt long-term.

Currently there are a number of victims of identity theft who may never recover from the crime [21]. Unless they are able to resolve all of the issues that have been created by the misuse, they will never return to the state that they had prior to the misuse. In some cases, the individual's ability to interact and participate in society may have been severely effected by the misuse of their identity. In order to understand why some victims continue to experience ongoing issues, and provide other victims with an improved or more efficient recovery; in-depth knowledge regarding the current problems and issues is required [30].

VI. Identified Issues within Australia

A number of issues have been identified in the research regarding victims of identity theft within Australia. The following section provides a summary of these issues.

A. Lack of centralized data collection

Currently, there is no centralized recording of incidents of identity theft within Australia. Unlike the United States that has the ITRC, there is no single entity collecting information regarding incidents involving the theft of another's identity.

The lack of data collection has a number of consequences, particularly on researchers in this area.

Firstly, it is difficult to ascertain the extent of identity theft within Australia. The studies that have been conducted report that the percentage of the population who may have been victims of identity theft could be between three to nine percent.

The lack of data also makes it difficult to conduct research in the area of identity theft victims. Without central data it is difficult to obtain an overall picture of the problem and to determine the efficacy of changes that have been made within organizations and legislation.

This issue has been raised by a number of researchers, government agencies and law enforcement agencies [14], [20], [31], [3] over the last decade, however no such service has as yet been established.

B. Assistance to Victims

Within the United States, in response to an increase in identity theft, the ITRC was established. The ITRC is a non-profit organization that provides assistance to victims as they work through the issues created by the misuse of their identity, provides resources for victims and also educates the public.

Currently victims within Australia are often required to take control of the issue themselves and work through the issues the organization(s) that are involved in the incident. The Australian Government Attorney-General's Department have published a brochure entitled "IdTheft: A kit to prevent and respond to identity theft" that provides victims with a list of things to do if they discover that they have been a victim of identity theft. The brochure also provides the contact information for a number of organizations that may be relevant. The kit focuses on victims of financial fraud and does not cover the many different ways that an identity can be misused. Although it has been identified that establishment of an Australian service similar to the ITRC is required [2], [25], [9], to date no such service has been established.

C. Legislative Changes

South Australia became the first Australian state to introduce specific legislation regarding identity theft in 2003. Since this time a number of other states have introduced their own changes. South Australia's legislation makes identity theft an offence, officially recognizes individual's who have had their identity misused by another individual as a victim of crime and includes the provision for a victim's certificate. The victim certificate does not require or compel an organization to take any action, it simply informs them that the person named on the document has been a victim of a crime involving their identity.

The aim of the victim certificate is to assist victims by providing them with official documentation recognizing their status as a victim of identity theft. In practice these certificates may provide little benefit for the victim and, in many cases, victims may not be able to obtain one due to the stipulation that a certificate may only be applied for once a perpetrator has been convicted of the specific offence. Victims often do not know who the perpetrator is and only a very small number of perpetrators are ever identified and charged with an identity theft offence [21]. Anecdotal evidence also suggests that a number of victims lose their right to apply for a certificate as charges relating to the identity theft are dropped during deal negotiations.

Little is known about the efficacy of these certificates, the number that have been provided since their introduction and whether victims of identity theft have even applied for them; currently no statistical information is available.

D. Identification Issues

The Theory of Human Identification, developed by Clarke [13], provides three means for making identifications of individuals, these being token-based, knowledge-based and biometrics. Historically, token-based forms of identification were predominantly used, however there recently have been moves towards the other forms and their combinations of the different means [13], [38]. Each of the different methods have been implemented in different ways, and each has issues which have been identified.

Primarily, tokens are used for identification in the format of documents. Within Australia, an individuals birth certificate, passport, drivers license, and medicare card are commonly used. There are a number of issues pertaining to tokens including the circular nature of documents, availability of forgeries, lack of security features, documents being used for identification that were not defined for that purpose, and stored information about these tokens being breached [23], [14], [39].

Knowledge-based identification is based on the premise that the individual being identified possesses knowledge that only that individual would know. Implementations of this type of identification have included usernames and passwords, "secret questions", and personal identification numbers (PINs). The reliability of knowledge-based systems has been found to be insufficient, especially in relation to the use of username and passwords [34]. There are many issues that have been identified including the selection of easy to remember passwords, using the one password for many systems, writing passwords down, and providing passwords to others [28].

Biometrics are based on the uniqueness of physical characteristics of the individual, are difficult to forge or change, and include finger prints, DNA profiles, and facial recognition [27], [1]. Biometrics have been used in a number of industries and for a number of purposes including access to automatic teller machines (ATMs), computer security, border security, and within law enforcement [1]. However there are issues regarding the use of biometrics including implementation issues, user and social acceptance, privacy concerns, and the issues of "function creep" (information collected used at a later date for a different purpose). Fingerprints are often seen to be aligned with criminal activity, including within Australia, which makes social acceptance difficult [35], [39]. One of the main issues is the requirement for the enrolment process to be infallible, otherwise the reliability of the system will be questioned [10].

Combinations of the three methods to identify individuals have also been used. The use of two-factor authentication methods is becoming more popular with many organizations, particularly in the financial sector. There are a number of different ways that two-factor authentication can be implemented, such as using a username and password along with the number that is displayed on a token which changes regularly. however even two-factor authentication is not infallible and already there are well documented cases of two-factor authentication being attacked in various ways including through the use of mobile phone porting, Man-in-the-Middle attacks, Trojan attacks, and through individuals sharing information with others [34].

Identification methods for individuals need to be verifiable, acceptable within society, able to be implemented easily and not open to compromise. The methods that are currently used within Australia are not infallible and this has lead to an apparent increase in crimes associated with identity, such as identity fraud, identity crimes, and identity theft.

E. Summary

Much of the research conducted within this domain has focused on Time 1 and Time 2, as yet there has been very little in-depth work conducted regarding Time 3 the outcomes of the misuse. Until this work has been done, there will be a gap in the knowledge and understanding of what is required to provide the support and assistance to victims.

A number of issues have been highlighted in this section, including the lack of research focus on Time 3. One of the main issues that has been identified by the studies conducted regarding victims of identity theft is that victims experience difficulties when dealing with the organizations involved. Depending on how the identity has been misused, there may be a number of different organizations that the victims need to interact with.

In order for a victim to be considered to be *recovered* from the incident, they should be provided with the assistance and information required to return to the state that they enjoyed prior to the incident taking place. As a victim may have been impacted by the crime in a number of different ways, there are can be a number of different aspects that the victim needs to deal with in order to achieve recovery including the legal, financial, mental, physical, health and behavioral. This research project will fundamentally deal with the legal and financial impacts that the victim experiences, and as an aside, will also obtain an understanding of the emotional impacts.

VII. This Research

The review of the literature indicates that research is required to obtain an understanding of Time 3. The main focus of this work to obtain an understanding regarding the interaction between the victim of the identity theft and the organizations that they deal with during the recovery process.

The following section provides an overview of the research currently being undertaken by the authors and provides the research questions, the methodology that will be utilized, details of the data that will be collected, along with the expected outcomes of the research.

A. The Research Questions

The main research question that this research aims to answer the following question:

- What do victims of identity theft experience as they work through the processes of recovery and what are the opportunities for improvement in processes and their experiences?

In order to answer this question, a number of sub-questions have been identified, these being:

- What pathways do victims of identity theft currently use during the recovery process?
- What processes do organizations currently use to assist victims of identity theft through the recovery process?
- What impact do the processes used by organizations have upon victims of identity theft?
- How effective are the current processes and what are the opportunities for improvement?

B. Methodology

This study is designed to explore how victims of identity theft work through the process of reestablishing their identity. This work will be conducted from a social constructivist perspective using a grounded theory methodology.

Grounded theory, part of the qualitative research methodology, was first described in 1967 by Glaser and Strauss in the book “The Discovery of Grounded Theory” [18]. Theories developed using grounded theory are said to be “grounded” in the data that is collected.

Four phases are undertaken when using a grounded theory approach, these being:

1) Research Design;
2) Data Collection;
3) Theoretical saturation; and
4) Discovery and Conclusion.

The first phase, Research design, involves defining research questions and selecting cases to be included. Phase two includes three parts, the collection of the data, the analysis, and the validation of the emerging theories. Data can come from a variety of different sources, with the most common source being interviews [41]. Other sources can include pictures, videos, and documents. Phase three is when theoretical saturation is identified. Finally, phase four is where the discoveries, conclusions and limitations of the study are defined [41].

Unlike quantitative studies, it is not possible to determine the number of samples, or in this case participants, prior to the study taking place. The aim of grounded theory is to keep adding new participants until saturation is reached. Theoretical saturation is reached when new data does not result in the emergence of a new category, categories are well organized and defined in regards to properties and dimensions, and the relationships between categories are validated and well established (see Figure: 2).

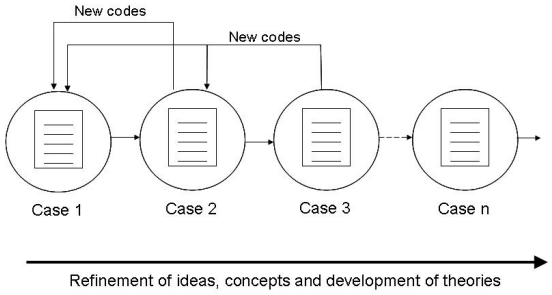

Fig. 2. Implementation of Grounded Theory

One of the distinguishing features of grounded theory, as compared to other qualitative methods, is the way in which the data is analyzed. Within grounded theory, the analysis is based upon the assignment of concepts and themes to the data (coding). The coding process contains three stages, these being open coding, axial coding and selective coding. One key concept of grounded theory is the *constant comparison* of new emerging codes with interviews that have already been coded. As the different interviews and cases are coded, new emerging codes will be discovered and the researcher then must re-visit the old cases to look for these new codes [5].

C. Data Collection

One of the main issues that has already been identified by this research is the lack of a centralized data collection of incidents of identity theft within Australian. Victims may be difficult to identify and after being a victim of identity theft they may be unwilling to participate in this activity. Victims may have also developed trust issues that may make them unwilling to participate if approached directly. In order to obtain an overall picture of the domain, the decision was made to collect data from three sources; these being victims of identity theft, target organizations, and reports of identity theft (see Figure: 3).

The primary source of data for this research project will be obtained from victims. Semi-structured interviews will be used to obtain information regarding what the victim experienced, what actions they undertook, who they contacted, and what obstacles they encountered after they discovered that their identity had been misused.

In order to obtain the perspective of the organizations that deal with victims, semi-structured interviews will also be conducted with investigators or personnel who deal with identity theft issues within target organizations. The target organizations that have been identified within the literature include financial institutions, utilities providers, insurance agencies, and government agencies [19]. Information regarding procedures that the organizations use when dealing with victims of identity theft will also be collected. This may include formal documentation, screen-shots, brochures, and flow-charts; these will be used as a reference point for the interview and also to be able to compare procedures used by organizations.

Finally, in order to obtain further details regarding incidents of identity theft, de-identified copies of reports will be obtained from law enforcement agencies, along with target organizations. The reports of identity theft will be utilized in a number of ways. Depending on what information the organization stores, the reports may contain both qualitative and quantitative information. The reports may contain narratives that will be able to be analyzed using the grounded theory methodology, along with other information (for example demographics) that may be analyzed using quantitative methods.

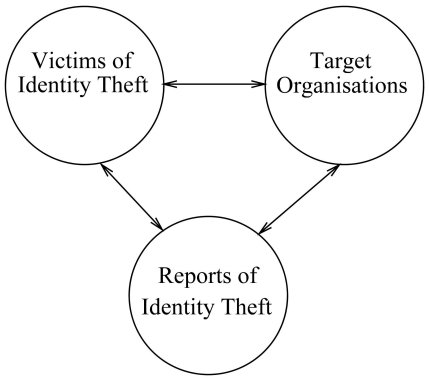

Fig. 3. Three data sources

VIII. Preliminary Work

A small number of victim stories (n=5) and one organization representative interview have been coded using Nvivo. From this preliminary work several themes have been identified that will be used in further work to be completed as a part of this study. These areas include how a victim discovers the misuse, the victims very first experience when dealing with the misuse, the impact of the misuse on the victim, information about the perpetrator, the victim's response and behavioral changes, the issues that the victim faces after the moment of discovery, and the response by the organization involved in the misuse.

Two victims discovered the misuse of their identity after being notified by their financial institution of unusual activity on their account (V2/V4). One victim had been informed of the misuse by an acquaintance who had found a profile of the victim on a social networking website (V1). In another case, the victim discovered the misuse after they were informed that someone using their identity was attempting to cash cheques that had been stolen (V5).

All of the victims experienced problems when dealing with the organization involved in the fraud and that their issues were not a high priority. A number of the victims felt that the organization did not care about their issues and that there was little follow up by the organization (V1/V2/V4). A number of victims (V1/V2) also felt that there were often delays and a lack of response by the organizations involved, including law enforcement agencies (V5).

Victims also questioned the motivations of the organization. One victim expressed that the organization did not really care about the victim and what they were experiencing, and that the organizations main focus was on recovering their losses (V4). V4 stated that "..all this credit card company cared about was recovering their funds". Victims also expressed that the organization did not appear to be interested in catching the perpetrator (V1/V2/V4), even when provided with the information by the victim. In one case the victim had provided the organization with details that they believed were pertinent to their case, however they reported that the organization had failed to follow up on the information (v2).

Emotionally victims were impacted in a variety of ways. Feelings of frustration, isolation and a change in reality were all reported. A small number of victims also indicated that the organization involved made them feel guilty and that they were in some way a part of the crime (V2). For example, V2 stated that they felt that the Law Enforcement Officer involved had "reached the conclusion that *V2* is guilty" . None of the victims experienced a physical impact directly from the crimes, however in one case the victim's mother experienced a physical reaction that was related to the stress experienced (V5). Financially two of the victims had been impacted directly by the crime, through a loss of money from their account. One victim indicated that they had been inconvenienced by the change in account numbers, when their old account had to be replaced by a new one; the victim had to spend time changing their details with other organizations.

The majority of the victims indicated that they could not be certain as to how the perpetrator obtained their personal information or who the perpetrator may be. Two victims indicated that they believed that it had been obtained from previous credit applications (V2/V4), another indicated that they may have been the victim of a phishing attack (V4), and one had their wallet stolen (V5). Only one victim believed that they knew who the perpetrator of the crime was. In this case, they felt that the perpetrator's actions had been driven by a vendetta (V1); the profile that had been created on a social networking website portrayed the victim in a very negative manner.

All victims indicated that their behavior had been changed by the experience. One victim, who had been a "loyal" customer of the organization prior to the incident, indicated that they would no longer continue to use the organizations services (V1). The incident also had an impact on how individuals felt about their personal identification information and the importance of protecting this information. In one case, the victim indicated that they decided against entering a competition as soon as they noted that the entry required them to provide personal identifying information that could be misused (V2).

Many victims also expressed concern about unknown issues or actions that the perpetrator may have undertaken. Victim V1 indicated that they were concerned about what else the perpetrator had done, who they had been in contact with, and how the perpetrator had portrayed them to others.

From an organizational perspective, it appears that the very first interaction the victim has with the organization can have an impact on the victim and how they deal with the issue. The following scenarios highlight two different ways in which the victim may discover the fraud and the different responses received.

1) The victim is informed of the fraud by the organization involved. During the initial conversation what has occurred is clearly explained and they are provided steps that the victim is required to follow in order to have the incident cleared from their record. The victim is normally willing to undertake the necessary steps.
2) The victim discovers the fraud themselves when they receive a bill for goods or services that they did not order. They call the organization involved, are transferred from one department to another, put on hold a number of times and are required to explain the problem to a number of different people, until finally being put through to the correct department. By this time, they may experience "Call-center rage" and when the representative of the organization explains that there is a set procedure that the victim has to follow the victim may react in a very negative way and be unwilling to undertake the necessary steps.

These two scenarios demonstrate the importance of the first contact with the organization. If it is handled poorly, it can exacerbate the experience of the victim, however if handled appropriately and if the victim is properly informed, the impact that the incident has upon the victim can be lessened.

One of the steps that the organization interviewed required from the victim was to make a police report. However, from the experience of a victim (V6) this can often be difficult. V6 attempted to report the crime to their local police station which refused to take their report as the crime had been committed in another state. V6 then attempted to report the matter to the local police of the state in which the incident was committed who also refused to take their statement as V6 could not make the report in person.

The preliminary work identifies some of the underlying issues that are faced by victims of identity theft including an apparent lack of understanding by the organizations involved, difficulties faced when trying to make reports to law enforcement agencies, and differences in the priorities of the victim and the organizations. The work also highlights the importance of the first contact that the organization has with the victim and that if it is not handled appropriately that it can impact how the victim responds to further requirements.

IX. Conclusion

This paper has provided an overview of identity theft, identified a number of issues regarding research in this area with a focus on Australia, highlighted the research that will be conducted as a part of this research project, and a brief summary of some of the preliminary work that has been conducted. This work highlights the need for further research

so that all victims of identity theft may be provided with the support and advice necessary to recover.

This research project is currently in the early stages of participant recruitment, data collection and analysis. The work discussed in this paper is only very preliminary work drawn from the analysis of a small number of cases. Before any conclusions can be made further work is required and is currently being undertaken.

ACKNOWLEDGEMENT

This research was conducted at the Internet Commerce Security Laboratory and was funded by the State Government of Victoria, IBM, Westpac, the Australian Federal Police and the University of Ballarat. More information can be found at `http://www.icsl.com.au`

REFERENCES

[1] K. F. Aas. 'the body does not lie': Identity, risk and trust in technoculture. *Crime Media Culture*, 2(2):143–158, 2006.

[2] ACPR. Australasian Identity Crime Policing Strategy 2003 - 2005. Electronic, March 2003.

[3] ACPR. Australasian identity crime policing strategy 2006 - 2008. Strategy, Australasian and South West Pacific Region Police Commissioners Conference, December 2005.

[4] ACPR. Standardisation of definitions of identity crime terms: A step towards consistency. Technical Report 145.3, Australasian Centre for Policing Research, March 2006.

[5] G. Allan. A critique of using grounded theory as a research method. *Electronic Journal of Business Research Methods*, 2(1):1–10, 2003.

[6] Australian Bureau of Statistics. Personal fraud. Technical Report 4528.0, Australian Bureau of Statistics, 2007.

[7] J. Benner, B. Givens, and E. Mierzwinski. Nowhere to turn: Speak out on identity theft. website, May 2000.

[8] S. E. Berg. *Crimes of the Internet*, chapter Chapter 12: Identity Theft Causes, Correlates and Factors: A Content Analysis, pages 225–250. Number 07458. Pearson Prentice Hall, 2009.

[9] J. Blindell. Review of the legal status and rights of victims of identity theft in Australia. Technical Report 145.2, Australian Centre for Policing Research, 2006.

[10] L. J. Camp. Digital identity. *IEEE Technology and Society Magazine*, 23 Issue 4:34 – 41, Fall 2004.

[11] Center for Identity Management and Information Protection. CIMIP Study Reveals New Findings About ID Theft Cases. Website: http://www.utica.edu/academic/institutes/cimip/mediacenter/index.cfm, May 2009.

[12] J. S. Cheney. Identity theft: Do definitions still matter? Discussion Paper August 2005, Fedberal Reserve Bank of Philadelphia, 2005.

[13] R. Clarke. Human idenficication in Information Sysems: Management Challenges and Public Policy Issues. *Information Technology and People*, 7(4):6–37, 1994.

[14] S. Cuganesan and D. Lacey. *Identity Fraud in Australia An evaluation of its Nature, Cost and Extent*. SIRCA, 2003.

[15] J. P. J. Dussich. Victimology - past, present and future. In *131st International Senior Seminar*, 2007.

[16] E. A. Fattah. Victimology: Past, present and future. *Criminologie*, 33(1):17–46, 2000.

[17] Galaxy Research. Identity Theft Report Prepared for: Veda Advantage. Technical report, Galaxy Research, April 2009.

[18] B. G. Glaser and A. L. Strauss. *The discovery of grounded theory; strategies for qualitative research*. Aldine Publishing Company, Chicago, 1967.

[19] R. D. Goldney. Victims of crime: A psychiatric perspective. *Psychiatry, Psychology and Law*, 5(1):153–157, April 1998.

[20] House of Representatives Standing Committee on Economics, Finance and Public Administration. Numbers on the Run. Review of the ANAO No.37 1998-99, The Parliment of the Commonwealth of Australia, August 2000.

[21] Identity Theft Resource Center. Identity Theft: The Aftermath 2008. Website, 2008.

[22] R. Jamieson, R. Sarre, A. Steel, G. Stephens, and D. Winchester. Defining identity crimes. In *Australasian Conference on Information Systems*, pages 442–452. ACIS, 3-5 December 2008.

[23] R. Jamieson, G. Stephens, and D. Winchester. Identity Fraud: The Player Landscape in Australia. In *18th Australasian Conference on Information Systems*, page 770, 5-7 Dec 2007.

[24] Javelin Strategy & Research. 2010 identity fraud survey report. Syndicated sample report, Javelin Strategy & Research, February 2010.

[25] J. Jefferson. Police and identity theft victims - preventing further victimisation. Current Commentary 7, Australasian Centre for Policing Research, April 2004.

[26] G. Jones and M. Levi. The value of identity and the need for authenticity. In *Turning the corner*. DTI Office of Science and Technology Crime Foresight Panel Essay, December 2000.

[27] D. K. N. Krishnan and D. R. Berwick. Developing a police perspective and exploring the use of biometrics and other emerging technologies as an investigative tool in identity crimes. Report 145.1, Australasian Centre for Policing Research, 2004.

[28] L. Ma, B. Ofoghi, P. Watters, and S. Brown. Detecting phishing emails using hybrid features. 2009.

[29] G. P. Main and B. Robson. Scoping identity fraud (an abridged version). Technical report, Attorney-Generals Department, September 2001.

[30] M. M. McNally. *Perspectives on Identity Theft*, volume 23 of *Criminal Prevention Series*, chapter Identity Theft and Opportunity, pages 33–55. Criminal Justice Press, Monsey, NY, U.S.A., 2008.

[31] Model Criminal Law Officers' Committtee. Final report identity crime. Final report, MCLOC, March 2008.

[32] G. R. Newman and M. M. McNally. Identity theft literature review. Technical Report 210459, U.S. Department of Justice, July 2005.

[33] Pearson. Product - Brief Symptom Inventory 18. Website: http://psychcorp.pearsonassessments.com/HAIWEB/Cultures/en-us/Productdetail.htm?Pid=PAg110, May 2010.

[34] B. Schneier. Two-factor authentication: Too little, too late. *Communications of the ACM*, 48(4):136, 2005.

[35] I. K. Sethi. *Privacy and Technologies of Identity*, chapter Biometrics: Overview and Applicaitons, pages 117–134. Springer Publishing Company Inc., 2005.

[36] T. Sharp, A. Shreve-Neiger, W. Fremouw, J. Kane, and S. Hutton. Exploring the psychological and somatic impact of identity theft. *Journal of Forensic Science*, 49(1):131–136, 2004.

[37] N. Shover and G. L. Fox. Long-term consequences of victimization by white-collar crime. *Justice Quarterly*, 11(1):75–98, March 1994.

[38] R. G. Smith. Identification processes in the higher education sector: risks and countermeasures. Technical Report 305, Australian Institute of Criminology, Canberra, December 2005.

[39] R. G. Smith. *Perspectives on Identity Theft*, volume 23 of *Criminal Prevention Series*, chapter Preventing Identity-Related Crime: The Challenges of Identification, pages 133–150. Criminal Justice Press, Monsey, NY, U.S.A., 2008.

[40] S. Sproule and N. Archer. Defining identity theft. In *Eighth World Congress on the Management of eBusiness*. IEEE Computer Society, 2007.

[41] A. Strauss and J. Corbin. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*. SAGE Publications, 1990.

[42] Wallis Consulting Group Pty Ltd. Community attitudes to privacy 2007. Technical report, Office of the Privacy Commissioner, Australia, Level 8, 133 Castlereagh St, Sydney, NSW, 2000, August 2007.