

Am I Who I Say I Am? A Systems Analysis into Identity Fraud in New Zealand

Mireille Johnson

A thesis submitted to Auckland University of Technology in fulfilment of the requirements for the degree of Master of Philosophy (MPhil)

2009

Institute of Public Policy

Primary Supervisor: Professor Marilyn Waring

Table of Contents

List of Figures	iv
List of Tables	v
Attestation of Authorship	vi
Acknowledgements.....	vii
Abstract.....	ix
1 INTRODUCTION	1
2 ETHICS	14
3 METHODOLOGY	18
3.1 SYSTEMS ANALYSIS	18
3.1.1 Introduction	18
3.1.2 Defining a System.....	19
3.1.3 Defining Systems Analysis.....	21
3.1.4 Applying Systems Analysis to Identity Fraud	22
3.2 KEY INFORMANT INTERVIEWING	27
3.2.1 Key Informants.....	29
3.2.2 The Interview Process	33
3.3 PARTICIPANT OBSERVATION.....	37
3.4 SECONDARY INFORMATION.....	41
3.5 REFLEXIVITY	47
4 LITERATURE REVIEW	53
4.1 CONCEPTUALISING IDENTITY FRAUD.....	54
4.2 THE NEW ZEALAND IDENTITY FRAUD ENVIRONMENT	57
4.3 IDENTITY FRAUD SYSTEM ISSUES.....	69
4.4 POLICY AND LEGISLATION	83
4.4.1 Policy	83
4.4.2 Legislation	96
5 FINDINGS.....	109
5.1 THE IDENTITY FRAUD ENVIRONMENT IN NEW ZEALAND	109
5.1.1 Trends	109
5.1.2 Issues.....	113
5.1.3 Main Threats	117
5.1.4 Abused Documents	121
5.2 SYSTEMS ISSUES.....	125

5.2.1 Identity Crimes and Documents	125
5.2.2 Identity Verification	129
5.2.3 Systems to Minimise Identity Fraud	140
5.2.4 Improvements in Systems to Combat Identity Crimes	147
5.2.5 Identity Fraud Cost and Statistics	149
5.3 FRAMEWORKS AND LEGISLATION	153
5.3.1 Frameworks	153
5.3.2 Legislation	157
6 CONCLUSION.....	164
REFERENCES.....	177
GLOSSARY.....	185
APPENDIX A – Auckland University of Technology Ethics Committee (AUTEC) Approval Memorandum	188
APPENDIX B – Participant Information Sheet	190

List of Figures

Figure 1: Percentage of Fraud Offences Resolved from 1999 to 2008. Adapted from <i>Fraud statistics from 1999 to 2008</i> , Statistics New Zealand, personal communication, June 30, 2009.	7
Figure 2: Number of Recorded Offences for Take/Obtain/Use Doc for Pecuniary Advantage from 1999 to 2008. Adapted from <i>Fraud statistics from 1999 to 2008</i> , Statistics New Zealand, personal communication, June 30, 2009.	8
Figure 3: Identity Fraud System Model	11
Figure 4: Fake Massey University Students' Association Webpage	63
Figure 5: Website - Fakepassport.cn	64
Figure 6: Website – Photobucket.com	65
Figure 7: New Zealand Identity Documents Displayed from a Google Image Search	66
Figure 8: New Zealand Passport Image and Personal Information Displayed Online	67
Figure 9: What Trends in Identity Fraud Have Emerged in New Zealand?	111
Figure 10: What Do You Think the Issues are Surrounding Identity Fraud in New Zealand? ...	114
Figure 11: Where Do You Perceive the Main Threat of Identity Fraud Comes from in New Zealand?	118
Figure 12: What Documents of Identity are Mainly Abused in New Zealand?	123
Figure 13: What are the Consequences to Your Organisation and the Public for Ineffective Identity Verification?	136
Figure 14: Does Your Organisation Have Best Practice Parameters Around Identity Verification?	139
Figure 15: What Improvements Would You Like to See in Your Organisation's Systems to Combat Identity Crimes?	148
Figure 16: How Much Has Identity Fraud Cost Your Organisation to Date?	151
Figure 17: What Do You Think About the Current Legislative Provisions for Identity Fraud Offences?	158
Figure 18: Capturing the Identity Fraud Environment in New Zealand - An Identity Policy Led Model	172

List of Tables

Table 1: Timetable of Interviews	31
Table 2: A Sample of New Zealand Related Identity Fraud Headlines.....	71
Table 3: New Zealand Legislative Acts Enforcing Identity Related Crime.....	96

Attestation of Authorship

I hereby declare that this submission is my own work and that, to the best of my knowledge and belief, it contains no material previously published or written by another person (except where explicitly defined in the acknowledgements), nor material which to a substantial extent has been submitted for the award of any other degree or diploma of a university or other institution of higher learning.

Acknowledgements

Final approval to interview my 15 key informants was granted by the Auckland University of Technology Ethics Committee (AUTEC) on 17 August 2007. The AUTEC reference number was 07/64.

In addition, I would like to acknowledge the support that I have received from various sources throughout the journey of this thesis:

I received financial support from my employer at Identity Services, the Department of Internal Affairs. The Department paid for my tuition fees and provided me with study leave to enable me to study part-time while continuing to work full-time. Additionally, they enabled me to travel to Wellington to interview key informants at times which complemented my other work commitments.

Auckland University of Technology, through the postgraduate research fund, paid for the use of my transcriber, Lorraine Dale. Lorraine listened to all recordings of my interviews with key informants and transcribed the interviews into a written format. I appreciate the amount of time that this took given her full-time work commitments.

Also paid from the University postgraduate research fund was Joy Oehlers from the University of Hawaii, who kindly double-checked my referencing in the thesis.

Ben Ashley and his graphics company, Benzine Design Limited, assisted me in professionally creating my vision for the Identity Fraud System Model. His company's quick interpretation and development of my 'amateur model' into a professional design was very much appreciated.

My thesis journey was made thoroughly educational and enjoyable by my two supervisors: Professor Marilyn Waring from Auckland University of Technology and Dr. Catherine Collinson from the New Zealand Police. Their subtle guidance, as well as their confidence and excitement in my work, was a highly motivating factor in a piece of work that I believed was important to be written in New Zealand.

Abstract

The purpose of this thesis was to research the systems issues surrounding identity fraud in New Zealand. There is only limited published research on the topic, either at an academic or industry level. The New Zealand Government has been conducting work in identity fraud in recent times but New Zealand appears to be lagging behind other similar westernised countries in terms of developing specific identity fraud policy or legislative provisions.

The research showed that New Zealand does have serious problems in its systems, which in some cases facilitate identity fraud. There is a lack of synchronicity between New Zealand Government systems which undermines a whole of government approach to minimising the risk of identity fraud. Issues in the private sector with identity fraud are just as serious, with financial advantage being one of the main reasons that identity fraud is committed. However, the lack of information sharing between the public and private sectors does not help stem the flow of identity fraud that is currently occurring.

Finding policy solutions to combat identity fraud is far from being simplistic. Public policy in this area is fraught with social, political and financial implications. Identity fraud is committed with speed while public policy faces a slow battle with red tape. Nonetheless, the New Zealand Government does not even appear to categorically know what is happening on its own door step with respect to identity fraud. There are no statistics on identity fraud and no concrete figures as to the cost of identity fraud to New Zealand. To compound problems, identity fraud is not even an official offence classification so even when it is occurring, it is not always being recorded.

The damage resulting from identity fraud can be catastrophic. Identity fraud is a breeder crime for other offences. It can enable an act of terrorism to occur, women and children to be trafficked, and organisations and individuals to suffer serious financial loss. In New Zealand however, the benefits of identity fraud can be great while the deterrents are weak. New Zealand faces potential harm to its international reputation if its systems are not strengthened to fight identity fraud. In order for this to occur, New Zealand needs to develop a specific identity fraud policy so that it has the basic knowledge in place to allocate the necessary resources to this problem.

1 INTRODUCTION

My name is Mireille Johnson. I was born in New Zealand but hold more than one nationality. I completed my undergraduate studies in Australia. But am I who I say I am? "Of course," you will probably say. You know that I must provide evidence of my identity to enrol in the Master of Philosophy programme and to obtain a student identification card. What you do not know is whether the identity that I provided the university was fictitious or not. I could be a KGB spy, a drug mule on the run from a cartel, a murderer who has escaped custody or an Al Qaeda convert. In all my years on this earth, I have never been stopped at any airport by any customs or immigration agency, and let's face it: I am not what they are looking for. I am a white female with blue eyes and rather non-descript features and unless I travel from a risky drug port such as Bangkok and I stand nervously in the Customs queue, sweating and playing with my clothes, I am an unlikely target for any government border agency. I know that government resources are limited and there are bigger fish to fry than me.

In order to enrol in this course I needed to provide a certified copy of my passport and academic record to the university. I could have purchased my Bachelor of Arts and Bachelor of Commerce degrees on the Internet. Alternatively, I could have borrowed my friend's qualifications and doctored them – chemical washing works a treat if you are careful. Besides, I know that university qualifications contain relatively unsophisticated security features and that because mine are from overseas and less familiar to the New Zealand eye, the chances of detection are relatively low. Moreover, getting documents certified is no problem as the people certifying them would have great trouble spotting a good fake. As for my passport, which could have been purchased on the streets of Kuala Lumpur, Bangkok, Guangzhou, Johannesburg,

Sao Paulo or even Frankfurt – the possibilities are endless. Naturally, I would have to be vigilant as to the quality of my forged passport as just one spot of glue reacting under ultra violet light during an examination could give the game away. If I plan correctly, I could arrange to land in New Zealand at peak time, when Customs officers at the primary line are often required to process 1500 passengers in just one hour. I could get even luckier, knowing that Customs had just recruited a substantial number of inexperienced, new staff. The odds of my walking through the airport border undetected are rather good.

Once I am in New Zealand, my new life as somebody else begins to be realised. I could take my forged passport or forged overseas driver's licence to AA and sit my testing for a valid New Zealand driver's licence. I know that the people behind the counter at AA are extremely unlikely to be trained in documentation examination and, even if they were, it is not an exact science and I doubt they would have the equipment to do the job anyway. Therefore, the chance of my not getting a New Zealand driver's licence is remote. Now that I have a validly issued New Zealand document that is often used as a form of identity, I can go down to the local department store and gain finance in my false identity. I know that even if the finance company is wary of me, they can check the validity of my New Zealand driver's licence and I will be fine. Alternatively, I can present them with my forged passport that I used to enter New Zealand on, as I know that they too will not be able to spot a fake – especially if it is a foreign passport. Moreover, as they are so keen to make a sale, they are unlikely to question me.

So my life in New Zealand evolves and I can open bank accounts, become a permanent resident, marry, join a gym, and buy a house, all as somebody else. Finally, by the time I apply to enrol in university, my false identity could be well established. Even if the

university checks with Immigration, my passport and bio data will be in their system as having entered New Zealand. The university will be happy with this as they will think that this is sufficient verification that I really do exist. After all, the university does not know that government records are not always testimony to the authenticity of a person. Besides, like the finance company, they too appreciate more business and if they wish to see more evidence of my identity, I always have that New Zealand driver's licence to show them. So now do you take it at face value that I am who I say I am?

The world of identity fraud and identity theft is not limited to the above scenario. Identity fraud transcends borders, governments, and commercial enterprises on this globalised planet. My own initiation into the identity fraud arena began in 2000, when I started work as an Immigration Officer for the New Zealand Immigration Service, now known as Immigration New Zealand (INZ). It was during my training at one of the visa and permit branches in Auckland that we had a visit from a senior Immigration Officer who worked for the Border and Investigations Branch (now the Border Security Group). She brought with her a pile of forged and counterfeit passports, which had been used by foreign nationals in attempts to enter or remain in New Zealand. These passports were from a variety of countries and to my untrained eye at that time, appeared genuine. During this training, I was introduced to my first ultra violet (UV) light and the benefits of its use in document examination. I immediately took the opportunity to duck under the table where it was darker with the UV light and discover what it was about these passports that were wrong. I was excited by the large differences in security features between passports from around the world and how counterfeiters attempted to beat the system. To this day, my interest in passport examination has not waned.

When a position became available to work for Border and Investigations at Auckland International Airport, I jumped at the opportunity. Despite my several years experience already in Immigration, the airport introduced me to another world – beyond that of honeymooners, business people and family vacationers. On my second day at the airport in the early evening, I had to escort two African males along with the police to their plane. They were being removed from New Zealand but were considered potentially too dangerous to be taken via the normal internal route to the plane. Six of us marched along the tarmac and up the external stairs of the air bridge before placing them in their seats. I felt like I was in a scene from a Hollywood blockbuster movie, feeling utterly naïve to think that this sort of thing did not go on in New Zealand. My naivety came to the fore once again when I was profiling passengers off a flight that had originated from Asia. I stopped a family and asked to see their passports but they told me that they did not have any – they only had forged ones that they had ripped up in the toilet on the plane en route to New Zealand. Naturally, over the following years, these events became quite familiar and commonplace to me. However, my time at the airport made me realise that New Zealand is not just a southern piece of land rather isolated from the rest of the world. It had become part of the globalised world and was not immune from its dark side.

After several years of dealing with people smugglers, refugees, prostitutes, drug mules, criminals and illegal workers at New Zealand's largest port, I decided to expand my horizons in the identity field. In 2005, I began work as an Investigator for the Identity Services business unit with the Department of Internal Affairs (DIA). It is here that I currently investigate fraudulent activity in the areas of New Zealand passport applications, New Zealand citizenship applications and birth, death and marriages registrations. While my previous focus at INZ had been on foreign nationals, my

experience at DIA has opened my eyes to fraud committed by New Zealand nationals as well. Their reasons for committing identity fraud can range in purpose from financial gain to running from the police to gang activities. Furthermore, Identity Services is in the business of managing New Zealand's most secure identity document – the New Zealand passport; and it is the custodian of the *Evidence of Identity Standard* (EOI) that was finalised in 2006 (New Zealand Department of Internal Affairs). This Standard aims to provide government departments with a uniform approach to authenticating an individual's identity and is linked to the e-government standards of authentication for online services.

It was during research for a university paper in 2005 on the EOI Framework (the draft of the Standard) that I contacted the National Bureau of Criminal Intelligence, which is part of the New Zealand Police. I asked the head of the Identity Intelligence Unit for some New Zealand statistics on identity crime. To my astonishment, he told me that there were no statistics and advised that he was currently trying to obtain funding to commission a research project into the economic cost of identity fraud in New Zealand. Additionally, he asked me whether I knew of anyone who would be willing to undertake such a study. However, both of the academic staff that I queried stated that it would be extremely difficult to accurately measure such fraud due to the intangible consequences as well as the lack of reporting (or knowing) of identity crimes. Nonetheless, the incidence of identity crimes has become more prevalent in the New Zealand media in recent times and they cross multiple sectors of the New Zealand economy.

A search online on 28 June 2009 with New Zealand's agency responsible for the collation of statistics, Statistics New Zealand, revealed that there were no results when

searching under the term “identity fraud”. I subsequently requested a *Customised Statistics Order* and was advised by email correspondence from Statistics New Zealand on 30 June 2009 that “unfortunately identity fraud or (sic) identity theft is not an official classification”. However, I was sent a breakdown of the Fraud statistics from 1999 to 2008. There were a total of 64 fraud offence categories, all of which had the capacity to include identity fraud (whether that is the manufacture of fraudulent items or the use of fraudulent items). Examples of these included:

- Counterfeits Seals/Stamps/Coin Etc
- Possesses Implements Not For Banknotes
- Imitating Authorised or Customary Marks
- Forges Cheque Over \$500
- Obtains by Cheque Over \$500 By False Pretence
- Obtains Other Service Through Credit By Fraud
- Breaches Social Security Act By Fraud
- Take/Obtain/Use Doc for Pecuniary Advantage
- Acknowledging Instrument – False Name
- Altering Etc Document with Intent to Defraud

From the figures held by Statistics New Zealand relating to fraud offences that had been recorded and resolved over a 10-year period between 1999 and 2008, on average, under half of the cases had been resolved¹. The average percentage of cases resolved in this period was 47.08%. The lowest rate of resolved offences was in 2002 with 43.49% resolved and the highest rate of resolved offences was in 2006 with

¹ Statistics New Zealand advised that these figures were independent of one another, in that the number of resolved cases was not calculated from the number of recorded cases in the same period. The resolved cases may represent recorded cases from previous periods.

51.04% of offences resolved. The following chart (Figure 1 next page) provides a graphic representation of the percentage of offences resolved over all 64 fraud offence categories:

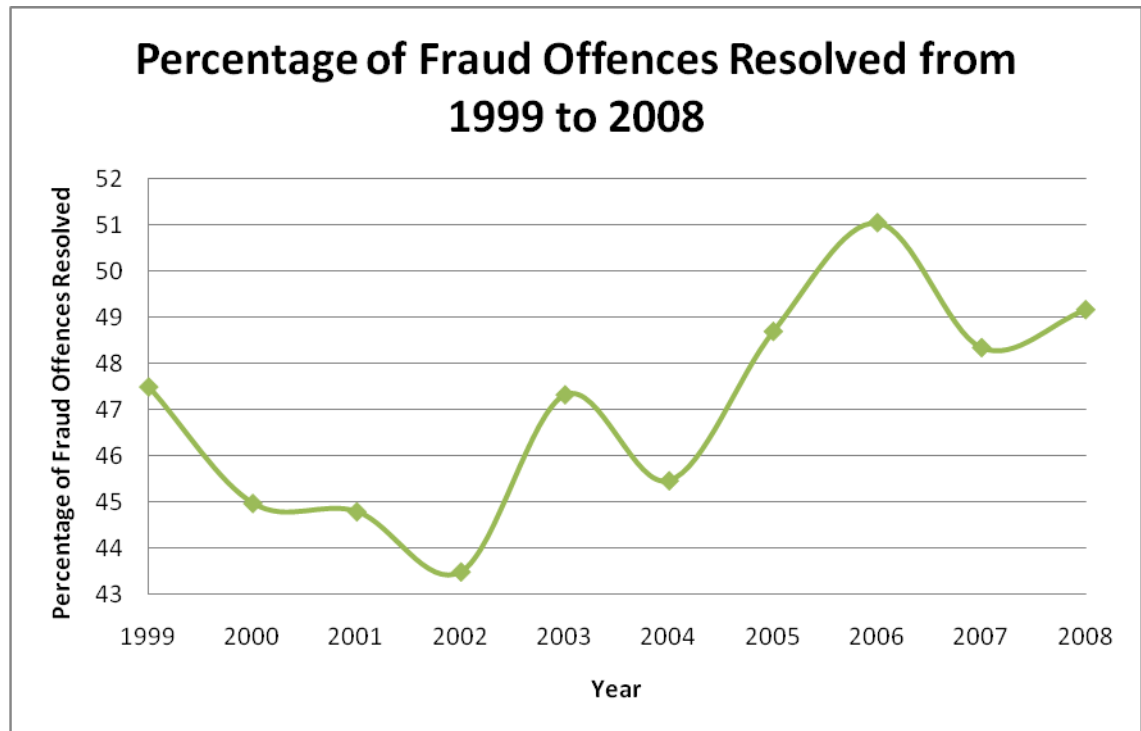


Figure 1: Percentage of Fraud Offences Resolved from 1999 to 2008. Adapted from *Fraud statistics from 1999 to 2008*, Statistics New Zealand, personal communication, June 30, 2009.

The offence category which had the most recorded offences over the 10-year period was *Take/Obtain/Use Doc² for Pecuniary Advantage*. This offence is often used by the Police for charging individuals with identity fraud related offences, such as the obtaining and use of a false passport. A total number of 99,655 offences were recorded between 1999 and 2008. The total of these offences that was resolved were 49,109, equating to a resolution rate of 49.28%. The number of offences recorded for *Take/Obtain/Use Doc for Pecuniary Advantage* has reduced considerably overall in the last ten years (see Figure 2 next page). The highest number of recorded offences was

² 'Doc' is an abbreviation for 'Document'.

in 2002 with 14,631 offences and the lowest was in 2008 with 5,611 offences recorded.

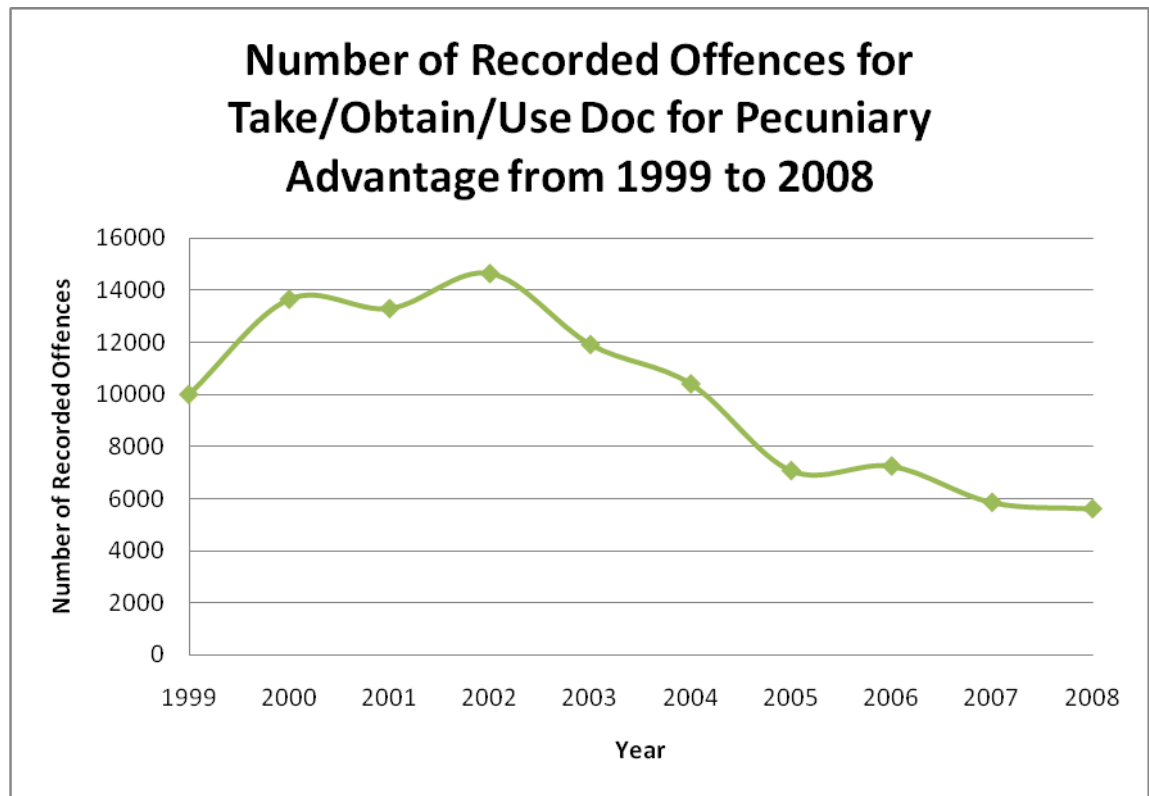


Figure 2: Number of Recorded Offences for Take/Obtain/Use Doc for Pecuniary Advantage from 1999 to 2008. Adapted from *Fraud statistics from 1999 to 2008*, Statistics New Zealand, personal communication, June 30, 2009.

To put in perspective, in the same 10-year period, an average of 79.16% of Violence offences were resolved, an average of 22.68% of Dishonesty offences were resolved and an average of 70.76% of Property Abuse offences were resolved (comparative to the recorded offences in the same year period). Across all offence categories (Violence, Sexual, Drugs and Anti-Social, Dishonesty, Property Damage, Property Abuse, Administrative) between 1999 and 2008, an average of 43.15% of all cases was resolved. Therefore, the average resolution rate of 47.08% for fraud offences was slightly higher than the overall average for all offences. Nevertheless, the average for all offences appears to be skewed towards a lower average of resolution due to the

very high number of dishonesty offences with a low resolution rate comparative to other crime categories.

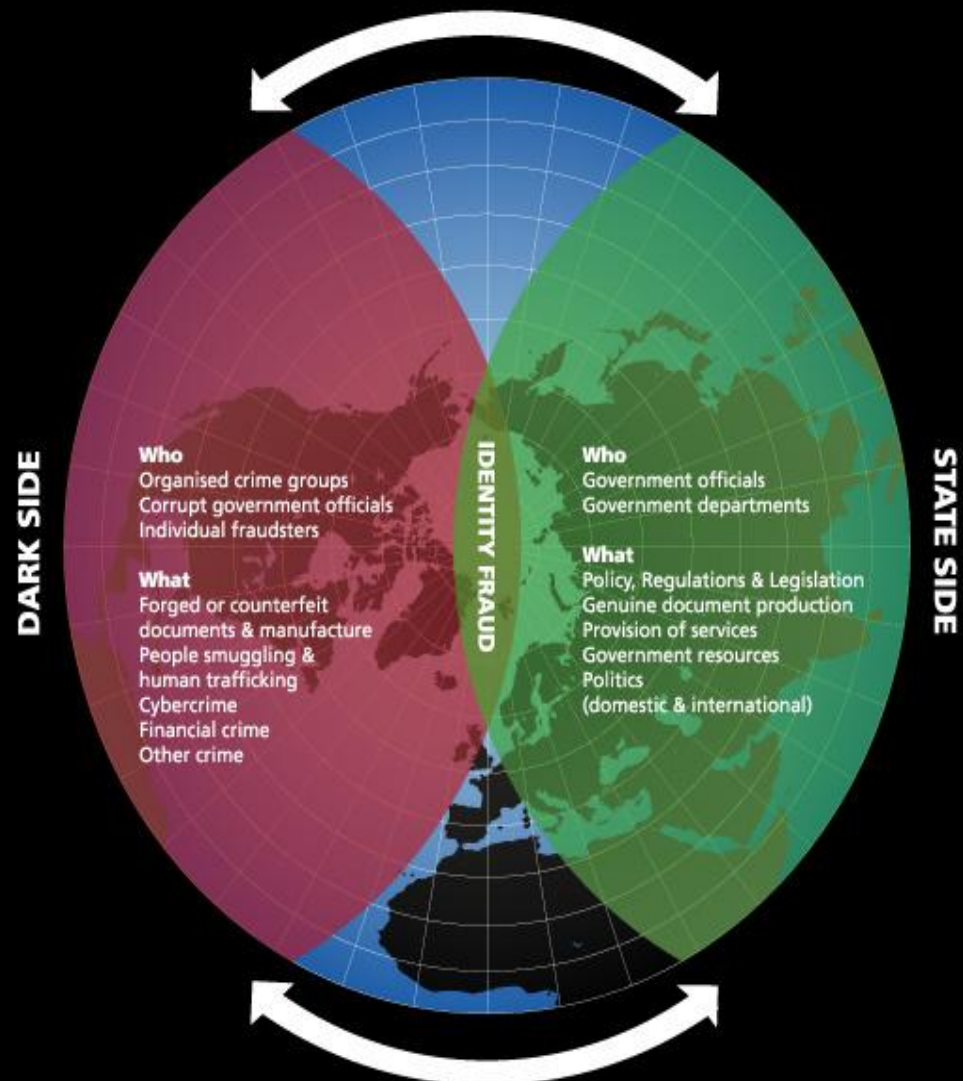
Due to the fact that identity fraud crosses industries and international borders (as well as criminal classifications), a systems analysis was employed as the methodology for this research. Triangulation was utilised in employing the following three methods in this research: participant observation, secondary information and reflexivity. The aim of this approach was to capture the systems weaknesses in respect of identity fraud that exist in both public and private sector organisations in New Zealand. The complexity of the identity fraud system can partly be attributed to the fact that it is made up of multiple subsystems which change according to the environment, the nature of the identity crime being committed, the modus operandi and the combination of elements in play, for example a forged or counterfeit driver's licence or passport. Therefore, no two situations involving identity fraud are ever the same. In an attempt to simplify what an identity fraud system is, I sought to develop a model which encompassed the generic elements of identity fraud and one that was simple enough to represent graphically. I was mindful that the model needed to provide a universal platform while at the same time acknowledging the global nature of identity fraud, the dynamic nature of identity fraud and the two sides of the identity fraud system, that is, the criminal side and the government side (see Figure 3 on page 11):

The Globe: Identity fraud permeates not just domestic but transnational borders. The international nature of identity fraud is represented by the globe in my model. However, the globe is not stagnant – it continually rotates in either direction, pivoting on identity fraud, bringing the Dark Side and State Side into contact with one another on an ongoing basis.

Dark Side: The “Dark Side” represents the criminal element of identity fraud as well as the unknown. Environmental influences such as political and religious persecution, economic disadvantage or outstanding criminal warrants can cause a person to obtain a false identity in order to escape their current situation. These factors, in turn, feed the organised crime groups who benefit financially from forged or counterfeit document manufacture, people smuggling and human trafficking; paying bribes to corrupt government officials who pave the way for the identity crime to be committed. Terrorism also threatens the national security of the State. As the globe turns, the Dark Side comes into contact with State Side and Dark Side practices are sometimes challenged. For example, the State may introduce new technology and policies at the border to prevent identity fraud. The terrorists or organised crime groups or individual fraudsters must therefore adapt, and find new ways or routes of entering a particular border.

State Side: “State Side” represents not only law enforcement but the whole of government of which law enforcement is a part. As the Dark Side comes into contact with the State, governmental policies, regulations and legislation adapt where appropriate. The State produces its own identity documents and is continually challenged by the Dark Side who tries to forge or counterfeit State documents. Thus, the State regularly updates security features in identity documents and their relative systems with the aim of preventing identity fraud from occurring. The State is further challenged by identity fraud from the Dark Side as the State is often the provider of primary governmental services for which identity verification is imperative. The Dark Side provides the impetus for the usage of law enforcement tools to combat identity crimes and for the collation of intelligence.

Identity Fraud System



Copyright © Mirella Giaccherini

Figure 3: Identity Fraud System Model

Given its diverse nature, identity fraud is a vast topic and as such, the research is limited within the confines of this thesis. Key informant interviewing was utilised in order to gain qualitative data on the topic from key informants in New Zealand whose work regularly involved aspects of identity fraud. The interview questions were divided into five categories: (1) trends, (2) systems issues, (3) privacy, (4) frameworks and legislation, (5) resolutions. Due to word limitations on this thesis, two of the categories were omitted from the Findings section. They were privacy and resolutions. The reason that I selected these two categories was because privacy, albeit an important issue in the development of databases to combat identity fraud for example, is not *directly* related to identity fraud systems issues in all circumstances. Notwithstanding this, privacy is mentioned in this thesis where necessary. The reason for omitting the resolutions section was because many of the systems issues discussed in the Findings section, inherently revealed the problems and, recommendations for policy development is covered in the Conclusion.

Topics considered relevant to identity fraud but not covered comprehensively in this thesis include:

Biometrics

Cybercrime

Forensic document examination

Identity management systems (including central databases)

National identification cards

Privacy

Technology developments

The thesis focuses on identity fraud systems issues in New Zealand and the appropriate public policy issues. It is divided into the following sections:

Chapter 1: Introduction

Chapter 2: Ethics

Chapter 3: Methodology

Chapter 4: Literature Review

Chapter 5: Findings

Chapter 6: Conclusion

2 ETHICS

In my research, I interviewed 15 key informants who were involved in working with identity fraud in the course of their work. As I intended to interview human participants, I needed to apply for ethics approval through the Auckland University of Technology Ethics Committee (AUTEC). I was granted ethics approval on 17 August 2007 (see Appendix A). According to the *AUT Postgraduate Handbook 2009* (p. 82), the key principles relating to ethics were as follows:

- Informed and voluntary consent;
- Respect for rights of privacy and confidentiality;
- Minimisation of risk;
- Truthfulness, including limitation of deception;
- Social and cultural sensitivity, including commitment to the principles of the Treaty of Waitangi;
- Research adequacy;
- Avoidance of conflict of interest.

Over the course of my research, five ethical issues needed to be addressed that fell within the bounds of the University's key ethical principles. These related to conflict of interest, privacy and intellectual property rights, consent of both key informants and organisations, confidentiality and, the minimisation of risk.

The first issue was the fact that my employer, Identity Services, the Department of Internal Affairs (DIA), was funding my research and their core business is identity. Identity Services had its own vested interests in the identity arena, as well as relationships with external stakeholders. My employer expressed concern that despite the fact that I was conducting independent student research, I was inextricably linked to DIA. Therefore, I was placed under a certain degree of pressure in the preliminary stages of my research to consider taking a direction that was amenable to DIA. Cheek (2007) warned of this possibility: "researchers must consider the potentially conflicting

agendas of funders, participants, and researchers” (p. 62). I maintained to my employer from the beginning that this research needed to be independent academic work and my supervisors contacted my employer to similarly advise. Cheek wrote: “Issues of control must be negotiated carefully in the very early stages of the research, as it is often too late once the project is well under way” (p. 63). After resolving this issue at the start of my research, there were no further problems in this respect throughout the rest of the research process.

The second ethical problem which arose was in the recruitment phase of key informants. One potential key informant referred my request to one of their internal researchers whose main concern was that I may misinterpret what the key informant stated to me in the interview. This obstacle was overcome by discussions with my supervisors, the internal researcher and me, where it was explained that I had personal experience in the field in which the key informant worked and that the key informant would have the opportunity to review their own interview transcript – thus the risk of misinterpretation would be minimised. The internal researcher also requested a copy of my findings prior to the completion of this thesis so that they could ensure that no misinterpretation had occurred. The internal researcher’s request for a copy of my findings prior to the finalisation of this thesis was declined as: (a) my findings would not be complete until my thesis was finished; (b) due to confidentiality considerations in line with the Auckland University of Technology guidelines relating to the release of data to a third party: “Students are strongly advised to consider issues of accessibility or availability of research data/materials, particularly those which may be restricted or confidential. This is to avoid any problems that may arise in the eventual publication of and public access to the thesis/dissertation” (*AUT Postgraduate Handbook*, 2009, p. 86). A further consideration was in relation to intellectual property. According to the

AUT Postgraduate Handbook, “students own the copyright in their theses as well as IP which they have created by themselves using their own resources and any University resources which are attributable to their course fees” (p. 88).

Thirdly, consent to participate in my research process was gained through individual consent forms (which were completed by the key informants) and organisational consent forms (which were completed by the person in the respective organisation that allowed me to interview their staff). Key informants were supplied with an information sheet which outlined the purpose of my research, the process in terms of their interviews and the management of the data that they would be supplying me with from their interviews (see Appendix B).

Fourthly, through the consent forms, the key informants and organisations advised whether they were willing for their names to be stated in the research or whether they wanted to use pseudonyms for reasons of confidentiality. However, the two forms were in some cases conflicting. For instance, it was possible for a key informant to state that they did want to be named but for the person authorising the interview to state that they did not want the organisation to be named and vice-versa. In the former situation, this meant that it would be relatively easy to identify the organisation that a key informant worked for if their real name was published. Four key informants had requested that their details be kept confidential, and there was a further one key informant whose name I kept confidential as a more senior manager had requested that the organisation’s name remain confidential.

The fifth issue was related to the minimisation of risk. There are security information issues associated with identity fraud. From the outset of this research I decided that I was only going to discuss publicly available material in this thesis. There is no classified

information in this thesis. In addition, in order not to prejudice any cases relating to identity fraud currently in the judicial system, these have not been discussed. In the course of my key informant interviews, one key informant made the request for me not to specifically name a programme in their organisation. This programme had been referred to by its specific name by several other key informants. Any reference to this programme in my thesis has been generic and not by name.

3 METHODOLOGY

3.1 SYSTEMS ANALYSIS

3.1.1 Introduction

Systems analysis was originally developed by the Rand Corporation in the United States of America and was used widely in military applications. Since its development, systems analysis has been applied largely in the scientific and engineering fields. In 1973, Brock, Chesebro, Cragan, and Klumpp commented that “the social sciences have begun to recognize the importance of systems analysis in descriptions and evaluations” (p. 26). However, the lack of literature on systems analysis in recent times suggests that its popularity has not been sustained. Nonetheless, Brannen (2004) states that “the aim of methodology is to help us *understand*” (p. 282). The complexity and nature of identity fraud in New Zealand, requires a rigorous and in-depth examination of the links in the identity fraud system which result in an identity fraud offence being successfully committed. In order to *understand* identity fraud at work, employing a systems methodology will ask: “How and why does this system as a whole function as it does?” (Patton, 1990, p. 78).

General systems theory provides the basis for systemic concepts; however, it incorporates a variety of different systems such as open and closed systems and concrete or abstract systems (Alter, 2007, p. 35). A systems analysis is required in this research in order to conceptualise the system of identity fraud and its parts in this globalised world. Skyttner (2005) refers to systems analysis as a method which takes “a strictly systemic outlook on complex organizations [and] can thus be considered an interdisciplinary framework of the common problem-view” (p. 42). Despite its strictly systemic outlook, systems analysis provides the opportunity for this research to examine all activities that facilitate identity fraud, whether they be legal or illegal, as

well as all environmental factors that are domestically or internationally based. Thus, as a methodology, systems analysis provides a large amount of flexibility to investigate all relevant issues at hand.

The following discussion in this section includes definitions of both a system and of systems analysis, followed by a more detailed discussion as to the applicability of systems analysis as a methodology to identity fraud.

3.1.2 Defining a System

Definitions of a system are varied and are inherently subjective. How one views a system is not necessarily the same as the next person's view and it is possible that one person may recognise a system while the next person does not. For example, a person that applies for finance using a false Australian driver's licence may appear as a one-off event to one finance company, however, another finance company may have seen this profile on more than one previous occasion and consequently, has recognised that there is a system to which this pattern of offending belongs. Thus, how one defines a system may be shaped by both knowledge and previous experiences. Skyttner (2005) supports this notion by stating that

A system is not something presented to the observer, it is something to be recognized by him Most often the word does not refer to existing things in the real world but rather to a way of organizing our thoughts about the real world. (pp. 56-57)

The German philosopher Fredrich Hegel (1770-1831) attributed the following generic characteristics to systems:

- The whole is more than the sum of the parts.
- The whole defines the nature of the parts.
- The parts cannot be understood by studying the whole.
- The parts are dynamically interrelated or interdependent. (as cited in Skyttner, 2005, pp. 49-50)

These four points can be applied to any system across a range of fields from education to zoology, however Stewart and Ayres (2001) advise that “a system is not a thing, and systems can begin to be defined only in relation to the purposes of the observer” (p. 81). Once again, this comment acknowledges that a systems definition is prey to subjectivity. To illustrate the point made by Stewart and Ayres, I turn to my experience as an Immigration Officer. On many occasions when a refugee has spontaneously sought asylum at the New Zealand border, after having travelled under a false name, I have viewed this refugee as having gone through the identity fraud system, that is, finding a helper to obtain forged documentation and facilitating their travel. From the refugee’s point of view, they have merely travelled through the refugee system, that is, they have done whatever they had to do to reach a safe country. My purpose in this example is to apply the legislation and policy to the illegal travel, while the refugee’s purpose is to save their own life. Similarly, Krone (1980) states that “systems are what people define them to be and what nature has bequeathed” (p. 17).

While Fredrich Hegel generically characterised systems, “Easton (1965) pioneered the application of systems theory to politics ... The chief attributes of the system Easton describes are environmental pressures and threats, program responses, information or feedback and effective adjustment” (Considine, 1994, p. 26). Nonetheless, Considine states that “systems are not living things which can make choices about their circumstances ... Systems are the patterns of interrelationships between actors” (p.27). In an identity fraud system, the actors are the politicians, the people smugglers, the fraudsters, the bank managers, the police, the customs officers, the immigration officers, the snakeheads³, the thieves, the con artists, the airline staff, the policy

³ The term ‘snakehead’ usually refers to a people smuggler in Asia who smuggles illegal immigrants from the People’s Republic of China. They are often associated with Asian organised crime gangs.

makers – the list is long and varied. Without the people smugglers paying a bribe to the immigration officers, without the con artists ripping off the bank managers, without the snakeheads making money out of the fraudsters, the identity fraud system would not automatically function or even exist.

3.1.3 Defining Systems Analysis

Being a systems analysis novice at the outset of this research, I became rather confused and disillusioned by the lack of definitions on systems analysis in the literature. Several books later Miser and Quade (1985) explained my misery by stating: “It is neither possible nor desirable to define systems analysis in concise and comprehensive terms. Since systems analysis deals with diverse problems and different contexts, it assumes many forms adapted to the problems, the systems, and their contexts” (p. 16). This brought me to question how I was meant to do a systems analysis into identity fraud without understanding the basic definition.

Krone (1980) attempts to generically define this problem by stipulating that: “Systems analysis is a set of techniques – qualitative, quantitative, and mixed – deriving its methodologies from the scientific method, systems philosophy, and branches of various scientific disciplines dealing with the phenomenon of choice” (p. 17). Krone continues:

My guess is that there are as many definitions for systems analysis as there are systems analysts. The frustrating thing about them all – mine at the beginning of this chapter included – is that none answer the question of “What is it?” in other than generalities. (p.19)

Nonetheless, a lack of a definition for systems analysis can be seen as an advantage, in that it provides the base for its flexibility and adaptability to such a wide range of disciplines, avoiding the need for researchers to fit a square peg in a round hole. This

does not mean that a flippant approach to systems analysis is appropriate as Hoos (1972) warns: “While lexical laxity can, perhaps, account for the myriad interpretations, broad and narrow, of *system*, only causal usage can explain the virtual interchangeability among *systems analysis*, *systems engineering*, and *systems management*” (p. 17). Much of this “interchangeability” among terms appears to be determined by the field in which one is researching, for example, information technology, business systems or biology. The purpose of my systems analysis research into identity fraud is to ultimately make public policy recommendations for action. In this regard, the aim of systems analysis provides a better picture as to what systems analysis is all about. Miser and Quade (1985) state:

The central purpose of systems analysis is to help public and private decision- and policymakers to ameliorate the problems and manage the policy issues they face. It does this by improving the basis for their judgment by generating information and marshaling evidence bearing on their problems and, in particular, on possible actions that may be suggested to alleviate them. (p.2)

3.1.4 Applying Systems Analysis to Identity Fraud

When I started to think about writing a thesis on identity fraud several years ago, I had problems ascertaining an appropriate methodology – even after having studied research methods for an entire year at university. The commonly recognised social science practices such as action research or focus groups do not have “the teeth” to meet the need of encompassing all of the variables in identity fraud to paint an accurate picture of the issues at hand. This is due to the fact that the identity fraud problem is multi-dimensional and because examining one part of the problem in isolation will not explain its existence, nor assist in developing public policy recommendations for the future. Moreover, due to the qualitative nature of this research, systems analysis is a relevant methodology as:

The predictive models for systems analysis must depend on a more direct use of judgment and intuition and less on quantitative relations. To achieve this dependence, human participants, usually experts or especially qualified people, are brought into the model structure. (Quade, 1985, p. 195)

Therefore, the use of systems analysis as a methodology complements the use of key informants as a method in my research.

Furthermore, identity fraud is a dynamic phenomenon for which systems analysis is an appropriate methodology as “clearly a systems analysis begins with the fundamental assertion that change is constantly occurring” (Brock et al., 1973, p. 35). “Change” in identity fraud variables take many forms: International conventions on human trafficking change; the *modus operandi* of identity fraud changes; immigration policies change; heads of States change; security features in documents change; regional stability changes; economic circumstances change; organised crime gangs change; technology changes; the price of a false passport changes – these are but a few examples. Even as I write this thesis, my own opinions on the subject change as identity fraud literature proliferates due to the growing media and public interest in the issue, causing governments around the world to respond quickly with solutions to what is seen as a serious global problem.

Easton (1965) states:

The only question of importance about a set selected as a system to be analyzed is whether this set constitutes an interesting one. Does it help us to understand and explain some aspect of human behaviour of concern to us? (p. 21)

At a personal level, identity fraud fascinates me due to its multi-faceted nature with multiple inputs leading to multiple outputs. Given the increasing levels of media interest, it appears that the subject appeals to the public as well – for the sake of one’s own personal security if nothing else. For law enforcement agencies, the interest lies in

the fact that identity fraud is the underlying foundation for the success in people committing other crimes – all in another identity; thus the risk to law enforcement agencies of not catching the offender is increased. A systems analysis also fulfils the second part of Easton's statement – it does assist in explaining human behaviour. An examination as to the inputs and environmental factors into the identity fraud system will provide an understanding as to why someone has committed an identity fraud offence. For example, the wars in Iraq and Afghanistan left parts of the populations displaced or in fear of their lives. Therefore, this factor was a major influence in nationals from those countries obtaining false documentation to flee to other safe countries. At the same time, for some, it was a convenient excuse for those nationals who had been living illegally in other countries even prior to the war occurring to gain false documentation and enter other countries illegally, as they now had a valid reason to claim asylum.

While identity fraud is commonly referred to as a problem, it is, in reality, a collective outcome from a number of problems and "it is common for a systems analysis to arise from a problem area or nexus of problems rather than a well-defined problem" (Miser & Quade, 1985, p. 17). Problems that give rise to identity fraud include loopholes in governmental policies, lack of international co-operation in law enforcement, lack of resources, jurisdictional hazards and the mere fact that no system is infallible. If one imagines a continuum with identity fraud being the centrepiece, it can be said that identity fraud then causes continual problems further down the continuum (or system) with other crimes being committed due to the existence of identity fraud in the first place.

Hoos (1972) states: “We must first recognise systems analysis as more than an assemblage of techniques and methods but rather as a social phenomenon fraught with social significance, perhaps all the more because it is characterized by contradictions, internal and external” (p. 241). The nature of identity fraud is consistent with the nature of systems analysis as described by Hoos. Identity fraud has become a social phenomenon, having infiltrated not only the public sphere but also private lives with the identities of individuals being stolen on a daily basis around the world. Its contradictions are many and varied. New Zealand is signatory to the 1951 United Nations Refugee Convention (United Nations High Commissioner for Refugees, 1951), yet the New Zealand Government places Airline Liaison Officers at offshore ports to prevent people who are holding forged documents from reaching New Zealand. These people are more often than not seeking asylum. Naturally, the New Zealand Government needs to be responsible in its immigration policies; however, being a United Nations signatory is somewhat a contradiction in the system. Therefore, systems analysis as a methodology mirrors the reality of identity fraud. Easton (1965) supports this notion by stating that systems theory “is merely an invitation to introduce additional elements to bring the theoretical picture closer to the empirical system” (p. 489).

More specifically in the law enforcement arena, Boguslaw (1982) comments that:

Difficulties in developing an adequate criterion for law enforcement can be traced on one level to the piecemeal approach which inevitably involves, to some degree, an abstracted view of the world. This abstracted view of the world is taken from a specialized perspective that implicitly ... ignores relevant considerations in the larger social system. (p. 43)

However, since Boguslaw made this comment in 1982, the world has become more globalised.

International law enforcement organisations such as Interpol or the World Customs Organisation now play a large part in connecting the global system of crime, including identity fraud. Easton (1965) recognises that there is an “international system”, stating:

The international system also has a regime. The relationships among the component actors are not random nor are their interactions entirely without constraints. Rules and expectations prevail, even though they may be less regularly complied with than in the many national systems. (p. 487)

In dealing with identity fraud in the international realm, non-compliance is evident in cases where the New Zealand Government has attempted to return passengers at the airport who, for instance, have arrived in the country on a forged passport. The New Zealand Government is a signatory to the ICAO Convention (International Civil Aviation Organisation, n.d.), as are 91 other countries around the world. Under Annex 9⁴ of this Convention, New Zealand may refuse entry to anyone holding a forged travel document and return them either to their country of citizenship or to the country where they last landed. In my experience as an Immigration Officer, there have been a number of cases where the country to which they are to be returned refuses to meet its obligations under Annex 9. The issue then becomes a diplomatic one. A systems analysis allows all relevant factors to identity fraud to be considered as part of the system, as Stewart and Ayres (2001) aptly state that “it is urban, environmental and crime issues which are most conducive to the systems approach” (p. 91).

Hoos (1972), however, warns that “Systems analysis, both as a process and a product, has not been subjected to sufficient critical analysis. This is because of the political

⁴ Annex 9 to the Chicago Convention “... embodies the Standards and Recommended Practices (SARPs) and guidance material pertaining specifically to facilitation of landside formalities for clearance of aircraft and commercial traffic through the requirements of customs, immigration, public health and agricultural authorities” (International Civil Aviation Organisation, n.d.).

nature of the environment in which the technique was spawned and proliferates” (p. 6). Hoos also goes on to say that “insistence on the distinction between theory and practice obscures the critical issues” (pp. 11-12). In considering the points raised by Hoos: (a) this research is being conducted at an academic institution and is free from the political interference that it may be subjected to in a workplace situation; (b) systems analysis may have proliferated by 1972, but as discussed earlier, its popularity has somewhat dwindled over recent years; (c) systems analysis enables theory to be closely aligned with the practical side of identity fraud in this research. Ultimately, the purpose of this thesis is to make practical and insightful recommendations for future public policy in identity fraud and the appropriateness of systems analysis in fulfilling this purpose is acknowledged by Brock et al. (1973) who state that “its flexible structure is such that it is capable of taking into account the most important elements of traditional decision-making as well as the new approaches ... making it a practical basis for public policy decision-making” (p. 17).

3.2 KEY INFORMANT INTERVIEWING

The purpose of the interview process in my research was to specifically: (a) uncover the current trends in identity fraud in New Zealand; (b) understand the current systems issues in identity fraud in the informants’ respective organisations; (c) establish whether New Zealand organisations are equipped to manage privacy concerns; (d) investigate current frameworks/legislation relating to identity fraud and (e) seek opinions from informants on possible ways to minimise the risk of identity fraud. Robson (2002) frankly states that “the interview is a flexible and adaptable way of finding things out” (p. 272). As mentioned earlier in this methodology chapter, identity fraud is a complex system. Therefore, the flexible and adaptable nature of

interviews in my primary data collection, maximises the opportunity to capture each facet of the identity fraud system.

In considering the appropriateness of face-to-face interviews as my primary data collection method, I ascertained what I wanted to discover in my research (as above). Other alternative methods included questionnaires and focus groups. However, I did not believe that a questionnaire (whether by mail or in person) could comprehensively cover the issues at hand because systems, as well as public policy are not always black and white and often, further explanations, clarifications or follow-up is required. Additionally, “mail questionnaires have the disadvantages of producing a potentially low response rate, being limited in length (with a restricted number of items) and having a high number of questions that are not answered” (McMurray, Pace, & Scott, 2004, p. 108). Moreover, I am not an expert in all areas of identity fraud and consequently, I may not ask all of the necessary questions in a questionnaire. Conversely, in an interview, I can expand my knowledge and the associated questions on an ongoing basis throughout the interview.

While focus groups do provide flexibility and adaptability to the researcher, this data collection method is used largely to generate *general* opinion on matters such as policy and commercial products. An investigation into systems of identity fraud is a *specialist* area as much of it is not in the public domain. Consequently, the numbers of people who are qualified to speak on this issue are limited and what they have to say may be sensitive, for reasons of national security or otherwise. In a one-on-one interviewing situation, if a piece of information is mistakenly revealed it can be quickly remedied, however, in a focus group situation “where information is shared with other participants there is no guarantee that they will respect each other’s confidentiality

later” (Gomm, 2004, p. 173). More importantly, the systems analysis methodology is the driving approach in this research. In order to achieve a systems analysis, specific information relating to the organisation in which key informants work is imperative. In a focus group situation, participants would not all be able to talk specifically on this issue as a group.

To date, in New Zealand, there appears to have been no specific research conducted in the identity fraud field, aside from the development of the Department of Internal Affairs led *Evidence of Identity Standard* (New Zealand Department of Internal Affairs, 2006). Rapley (2004) states that “interviewing can be used as a way to enable previously hidden, or silenced, voices to speak” (p. 25). My interviews, therefore, provide a vehicle for discussion of identity fraud and verification systems in New Zealand that have previously not been heard. However, while interviewing is an effective tool in qualitative research, a range of issues must be considered, from the selection of key informants through to the interview process and subsequent follow-up. This section firstly discusses the use of key informants and secondly examines the issues in interviewing them.

3.2.1 Key Informants

The applications of identity fraud are diverse across industries. Every offender has his or her own agenda for committing an identity crime. My own personal knowledge and observations are limited to those areas in which I have worked. For this reason, I employed key informant interviewing as one of my research methods to assist me in understanding the systems of identity fraud at play in New Zealand, across both the private and public sectors. In this regard, Patton (1990) supports the use of key informants, stating: “One of the mainstays of fieldwork is the use of key informants as

sources of information about what the observer has not or cannot experience as well as a source of explanation for events the observer has actually witnessed” (p. 263).

A primary consideration was to establish how many key informants to interview so that I would be provided with a significant and accurate picture of identity fraud systems in my data. Burnham, Gilland, Grant, and Layton-Henry (2004) state, “There is no simple answer to this question, as in large it should be determined by the objectives and purpose of your study” (p. 207). At the outset I intended to interview at least one representative from each Government organisation in New Zealand that deals with identity fraud on a daily basis, as well as a selection of private organisations and international agencies. However, the final number of key informants that I interviewed was partly determined by time and cost.

In respect of time, the recruitment of key informants to interview is a process that can take a considerable amount of time in itself. In my research, I interviewed a total of 15 key informants. Of these 15 key informants there were nine that I was personally aware of through my current and past employment; there were four whose names were given to me by other contacts that I had; there were two that I was made aware of through the media. Due to contacts from my past and current employment and due to the lack of New Zealand research into identity fraud, I found that most of the people whom I approached were amenable to participating in my research. The two exceptions to this were the Ministry of Social Development who declined to be interviewed and the Accident Compensation Corporation who expressed initial interest but then did not respond further to my invitation. Burnham et al. (2004) warn that “gatekeepers” may be encountered in organisations: “In order to gain access to such institutions, it is often necessary to negotiate with gatekeepers who may deny access

to the institution, ration it, or impose conditions on the way in which the research is carried out” (p. 259). As discussed previously in the Ethics chapter of this thesis, the only encounter with a gatekeeper was with a researcher from one key informant’s agency.

The following table (Table 1) provides an outline of the dates I interviewed my 15 key informants, the city that they were interviewed in and the number of key informants interviewed in the respective periods:

Table 1: Timetable of Interviews

INTERVIEW DATES	LOCATION	NUMBER
20-21 September 2007	Wellington	3
14-16 November 2007	Wellington	5
11 March 2008	Auckland	1
7-8 April 2008	Wellington	4
31 October 2008	Auckland	2

There were several factors that impacted upon the timing of interviews. Firstly, the majority of these key informants hold senior positions in their organisations and hence, they are very busy people. In this vein, Burnham et al. (2004) state that the accessibility of key informants is a potential hurdle as “such individuals are usually very busy and they have to be provided with some convincing motivation for seeing a researcher” (p. 208). Moreover, Spradley (1979) advises that “the needs of informants for some gain from the project must not be ignored” (p. 25). Therefore, I offered key informants, via the Participant’s Information Sheet, a summary report of my research at the conclusion of this thesis. From the 15 key informants, 13 requested a summary report and 2 did not request a copy. Additionally, some were willing to donate their time due to the lack of identity fraud research in New Zealand and some because they knew me. Secondly, compounding the timing issues of interviews was the fact that I

reside in Auckland while 12 of my key informants were based in Wellington. This meant I needed to co-ordinate as many key informants as possible for a two to three day trip to Wellington. Thirdly, my own work and personal circumstances impacted upon the scheduling of interviews, at one point causing a two month delay in the progression of my field work.

In respect of cost, there were two factors to consider. Firstly, I was fortunate that the cost of travel to Wellington was covered by my employer but I had a responsibility to minimise the number of trips and the time spent there. At times, my interviewing in Wellington was scheduled in conjunction with other work commitments. Secondly, due to the fact that I work full-time and my spare time is minimal, I employed a transcriber to transcribe all of my key informant interviews. The payment of the transcriber came from a fund that the University allocates to me each year for costs towards postgraduate research. Therefore, the number of interviews was also limited by cost in this regard.

However, time and cost aside, I wanted to ensure that I captured a diverse range of qualitative identity fraud data across the public and private sectors. Patton (1990) warns that “the danger in using key informants is that their perspectives will be distorted and biased, thus giving an inaccurate picture of what is happening” (p. 264). I minimised this risk of data contamination in my research by selecting a range of key informants who, although may work in similar fields, are employed by different organisations. The aim of this approach was that I would ultimately obtain an environmental picture of systemic issues and patterns in identity fraud in New Zealand. Additionally, I mitigated the risk of bias by interviewing key informants who have a real working knowledge of identity fraud in New Zealand. I was mindful that

managers may have the authority to speak on this topic but may not be aware of the operational and frontline issues at hand. An in-depth knowledge held by key informants of systemic issues and trends in identity fraud was imperative and I anticipated that the cross-industry participation of key informants would provide greater texture to my data.

3.2.2 The Interview Process

Prior to interviewing my key informants, I developed a pilot interview template in order to ascertain whether my questions would elicit a full and open response and, whether it was an appropriate length time wise. I decided to ask a number of standard questions of all key informants, so that a consistency in the data could be achieved for comparative purposes. However, a low level of rigidity during the interview was important as I wanted information to flow freely from the key informants. Encouraging this sort of dialogue would assist in filling my own knowledge gaps and giving me further direction in my research. Burnham et al. (2004) reinforce this notion: “With semi-structured interviewing, the researcher can redesign the questions as the research proceeds to take account of new themes” (p. 216). The interview questions that I developed for my pilot interview were grouped according to five themes: (1) Trends; (2) Systems Issues; (3) Privacy; (4) Frameworks/Legislation; (5) Resolutions. Robson (2002) supports this approach by stating: “Interviewers have their shopping list of topics and want to get responses from them, but as a matter of tactics they have greater freedom in the sequencing of questions, in their exact wording, and in the amount of time and attention given to different topics” (p. 237). Accordingly, I devoted more questions in relation to system issues as this is the focus of my research, as well as being an area in which I needed to obtain greater understanding from my key informants about their organisational processes. My initial set of questions and

themes that I developed for the pilot interview, were based upon my own knowledge and reading of the literature to date. Tolich and Davidson (1999) similarly state: “The initial interview guide – the questions, the themes and prompts – is generated from what researchers know from their general knowledge, from what informants have told them, and/or from a literature search” (p. 257).

On 12 August 2007, my pilot interview was conducted with the assistance of my transcriber as interviewee, as she had a basic understanding of identity fraud through her previous employment. In terms of timing, my pilot interview with her took 57 minutes and 49 seconds. My aim was to interview for a period of approximately one hour so this fell within acceptable limits. In addition, my transcriber was able to provide feedback on the content of my questioning at which time she thought that the pilot questions covered all areas within the objective of my thesis. There were some questions that she struggled to answer, but I expected that to be the case as she has not worked directly in the identity fraud field.

While Patton (1990) warns of bias on the part of key informants (p. 264), Rapley (2004) warns of the challenge faced by interviewers in relation to neutrality (p. 20). During the interview, I was careful not to ask any leading questions and I provided key informants with the opportunity to answer the majority of questions in an open-ended format. Jorgensen (1989) recommends asking “descriptive questions” as they “explore the general contours of some matter in fairly comprehensive detail” (p. 86). Nevertheless, despite the best attempts by both interviewer and key informant to remain objective during the interview, there will never be a perfect balance of neutrality. Qualitative data is inherently subjective and defining ‘neutrality’ is subjective per se. Rapley (2004) similarly comments: “Actually ‘*being neutral*’ in any

conventional sense is actually impossible ... Interviewers have overarching control, they guide the talk, they promote it through questions, silence and response tokens” (p. 20). After reading my interview transcripts, it was evident that despite my best intentions I had asked some leading questions; albeit a minimal number. However, the semi-structured nature of my interviews promoted a balance between both the key informants and I, allowing both sides to speak where appropriate and thus minimising bias.

Interviews also minimise the risk of misunderstandings, as they provide the opportunity to meet with the interviewee in person and read their body language in line with their responses. Furthermore, Tolich and Davidson (1999) advise, “As well as verbal prompts, prompts come in many forms. Body language prompts, such as a raised eyebrow, gesturing with open hands, a cough, or deliberately leaning forward, all help to elicit more information when you are seeking a fuller answer from the informant” (p. 262). Additionally, Schutt (2006) states that “respondents’ interpretations of questions can be probed and clarified” (p. 268). I noted the advantage of this in my pilot interview, where the interviewee sometimes did not provide an answer that was clearly linked to my question. Her body language also indicated that she was finding it difficult, in some cases, to answer the question and I used this as my prompt to step in and re-explain the question in a more specific manner. At the end of the pilot interview, I asked my interviewee whether she thought that the questions were clear, as I thought that I may have to re-write some of the questions that she had difficulty in answering. To my surprise she said that they were all clear. In evaluating this response, I concluded that perhaps she did not know the answer to all of the questions, but felt compelled to give me an answer as I was interviewing her in person. Therefore, face-to-face interviews may be detrimental in

this respect. Schutt noted this in relation to sensitive topics: “The presence of an interviewer may make it more difficult for respondents to give honest answers to questions about sensitive personal matters” (p. 269). In my pilot interview, it was possible that my interviewee did not want to feel humiliated by merely stating that she did not know the answer. The consequences of this are that data collected during an interview may not be reliable and to minimise this risk in my research, I advised all interviewees, before the interview began, that if they did not know the answer to a question to advise me accordingly. This strategy was effective in my interviews as key informants readily told me if they were not able to or could not answer a question. Their reasons for not answering questions ranged from a lack of knowledge to anxiety in expressing their own opinions versus their organisation’s stance on certain matters. Finally, on the method of data recording during an interview, there are two main approaches: audio/video recording and note-taking. May (2001) states that:

Tape recording can assist interpretation as it allows the interviewer to concentrate on the conversation and record the non-verbal gestures of the interviewee during the interview, rather than spending time looking down at their notes and writing what is said. (p. 138)

However, the disadvantage of this recording method is that interviewees may not feel safe to say what they really think and that technology may fail during the interview. In fact, Jones (2002) advocates for note-taking at the expense of social interaction, by stating:

Although there is some debate about the possible reduction of eye-contact which might result from note-taking, this can combat the fear that the batteries in tape recorder have run down and provide a good back-up in the event of technical problems. (p. 207)

Too much of a focus on note-taking can also detract from actively listening to the interviewee, as I discovered in my pilot interview. For the first half of the interview, I

was writing down nearly everything that was said, partly due to occupational habit. I realised that I was missing non-verbal prompts and opportunities to ask more questions based upon my respondent's answers. In order to combat my fear of failing technology with my key informants, I recorded my interviews with two different machines thus creating a backup and putting my mind at ease. The use of two machines meant that I could be less stringent in note taking (although I always noted the main points) and focus more on what the key informants were telling me which in turn, enabled me to ask more follow-up questions.

Overall, I gathered a good amount of information from my 15 key informant interviews. The interviews ranged in length from approximately 47 minutes to 1 hour and 25 minutes. I received comments from several of my key informants after their interviews that my questions comprehensively covered the issues in identity fraud and the majority of key informants did not add anything further when they were given the opportunity to do so at the end of their respective interviews.

3.3 PARTICIPANT OBSERVATION

Definitions of participant observation are varied in length between commentators. Loftland and Loftland (as cited in Burnham et al., 2004) simply define participant observation as “ ‘a process in which an investigator establishes a many-sided and relatively long-term relationship with a human association in its natural setting for the purpose of developing a scientific understanding of that association’ ” (p. 222). In this research, my participant observation of identity fraud has occurred over a period of nine years while working for Immigration New Zealand and the Department of Internal Affairs. This method of participant observation is not considered to be the norm.

Delamont (2004) states that “the term ‘participant’ observation does not usually mean real participation” (p. 218) but more an observation of how people participate. Spradley (1979) further defines the participant by differentiating between what he calls the “participant observer” and the “ordinary participant” (p. 54). Similar to Delamont’s notion of participant observation, the participant observer enters a social setting with the purpose of participating in relevant activities *and* observing the environment in which these activities occur. In contrast, the ordinary participant merely participates in the activities without recording descriptions of the people, the environment or the activities involved. My own experiences, therefore, are consistent with Spradley’s “ordinary participant”. However, while I have not kept a personal diary over the years relating to incidences of identity fraud in which I have been involved, there are cases that have stood out in my mind due to their nature, timing, the character of the offender and/or the amount of time I have spent on them. Some examples of these include the pregnant Nigerian woman who arrived at the airport on Christmas Eve on a falsely obtained Australian passport that stated that she was 14 years old; the young, blonde, long-haired ‘Greek’ backpacker who was in fact an Albanian on a forged Greek passport and who popped his head in the office door to say to me “Good job!” as he was being taken to his plane for removal.

Delamont (2004) argues that “anything not recorded is lost” (p. 225). I acknowledge that my memory of events will not be as detailed as if I had made notes of observations at the time, however, while working at Auckland International Airport, the environmental variables remain rather constant: the physical environment was the same, the actors were usually the same (airline staff, Customs Officers, Police Officers and Immigration Officers) and the outcomes were limited in numbers due to policy and practice restrictions. Moreover, due to the risk of identity fraud or other

immigration related issues, a large part of my job was profiling passengers and observing behaviours on a daily basis. I came to learn how to identify potential illegal workers such as prostitutes, chefs or orchard workers by the way they walked towards passport control, the way they completed their arrival card, the way they pretended to be alone when they were part of an organised group. Spradley (1979) supports this point, stating that “the goal is to select a social situation in which some activities frequently recur” (p. 50). This was true of my time at the airport and while I did not maintain a personal diary, I was required to keep an ‘airport log’, which was an electronic log of events and behaviours that occurred while on duty. This practice encouraged reflection on a daily basis. Therefore, in line with Spradley, “All human beings use their perceptual skills to gather information about social situations. We are all *observers*, even when acting as ordinary participants” (p. 56).

Burnham et al. (2004) state that one of the downfalls of participant observation is that “A single researcher or even a team of researchers can only observe a certain amount” (p. 235). Standard participant observation only allows the participant observer a snapshot of activity over a limited period of time. In addition, in the identity fraud area, it is unlikely that an ‘outsider’ would be given the authority to observe frontline occurrences of identity fraud due to the security environment in which it occurs, privacy concerns, diplomatic concerns, national security concerns and/or the security status of the information received. Jorgensen (1989) describes the participant role on “a continuum from that of *complete outsider* to *complete insider*” (p. 55). Given my work experience in identity fraud, I fall within the “*complete insider*” realm and my immersion in this field has shaped my beliefs and behaviours on this topic.

While Spradley (1979) would argue that my observations have been experienced in a “subjective manner” as an insider and an ordinary participant (p. 56), I contest that my observations have been made based upon participation in real-life activities and as a result, my understanding of identity fraud is not based merely upon observations but also interactions. Jorgensen (1989) supports this notion: “In the course of daily life, people make sense of the world around them; they give it meaning The world of everyday life constitutes *reality* for its inhabitants, natives, insiders, or members” (p. 14). In my work, my reality has provided me with a 360 degree view of identity fraud in action. While it can be argued that I have only worked for the Government in this area and therefore, have a one dimensional view of this topic, I am human and have experienced much more than merely applying government policies. I have heard both inconsequential and devastatingly sad stories from the people that have committed identity fraud. I have watched them break down as I delivered them to the police station to be placed in custody; I have seen them so stressed during interviews that an ambulance call was needed for their chest pains; I have had them begging me not to send them back home as they felt as though they had let down not only their families, but their whole village. No human being is immune from observing this type of emotion. In contrast to Spradley (1979), Jorgensen (1989) states that, “Accurate (objective and truthful) findings are *more* rather than less likely as the researcher becomes involved directly, personally, and existentially with people in daily life The potential for misunderstanding and inaccurate observation increases when the researcher remains aloof and distanced physically and socially from the subject of study” (p. 56). My personal experience has been neither distance nor socially removed.

Participant observation is not only an appropriate method in this research, but is of extreme value as “participation is a strategy for gaining access to otherwise

inaccessible dimensions of human life and experience” (Jorgensen, 1989, p. 23). As previously stated, the web of identity fraud is complex and tangled, hence the necessity of systems analysis as a methodology. Consequently, such a complex system requires an insider’s knowledge as identity fraud is not just about the fraudulent identity document in front of you. It is imperative that for any study in this area, the researcher has a good understanding of the processes and systems involved. In my own experiences in observing the emotions of an offender, it is not just because they were caught – it is about the journey that they had embarked on to reach their destination. This journey is both physical and emotional with the offender having to endure sometimes days or months of travel, knowing at any point they could be arrested, knowing that they have a family to protect, for example. A standard participant observer would not have the necessary depth of understanding or insight to accurately report all the facets of this system without experiencing it first hand. In this vein, Atkinson and Hammersley (1994) state: “because we cannot study the social world without being a part of it, all social research is a form of participant observation” (p. 249).

3.4 SECONDARY INFORMATION

Secondary information is the third part of triangulation in this research. It supports my primary data collected through key informant interviews and my own participant observation by: (a) providing a backdrop to the environment in which identity fraud has emerged; (b) providing statistics in identity fraud; (c) describing trends in identity fraud; (d) reporting strategies from around the world to combat identity fraud; (e) reporting issues in identity fraud; (f) describing the impact of identity fraud. Stewart (1984) states that “more often, primary and secondary research are used in a

complementary fashion, rather than as substitutes for one another” (p. 12). Secondary sources of information in my research include annual reports, statements of intent, media articles, media releases, books, journal articles, academic reports, commercial reports, international and domestic statistics and government reports. Corti and Thompson (2004) support the use of such documents in research by stating that “a collection may also contain ‘secondary’ sources utilized for a particular research study, such as newspaper clippings and organizations or medical records” (p. 328).

In defining forms of secondary research and information, there is more than one term to consider. Terms such as secondary sources, secondary information, secondary data and secondary analysis are all commonly used in the literature. Kelsey (2001) defines *secondary sources* as “a generic term that describes research where no new primary data are collected, but new interpretations (and conclusions) are drawn from existing data” (p. 309). Stewart (1984) defines the aforementioned other three terms, stating that:

The term *secondary* information is frequently used to refer to both secondary data (the raw data obtained in various studies) and secondary sources (the published summaries of these data) ... the distinction among these types of information tend to blur in practice. The use of secondary information is often referred to as *secondary* analysis (or research). Secondary analysis is simply a further analysis of information that has already been obtained. (p. 11)

In this research, a combination of both quantitative and qualitative secondary sources will be utilised. However, although there are advantages to utilising this information I am mindful of the inherent disadvantages.

At the outset of my research, secondary sources have assisted in shaping the direction of my primary data collation through key informant interviews. Such secondary sources as annual reports, media articles and releases have helped me identify the

knowledge gaps in identity fraud in New Zealand and I have structured my interview questions accordingly. Stewart (1984) concurs, stating: “Secondary research helps define the agenda for subsequent primary research by suggesting which questions require answers that have not been obtained in previous research” (p. 13). Nonetheless, caution is needed when considering published secondary information as “much secondary analysis uses data for purposes other than for which they were collected” (Hinde, 2002, p. 252). This raises issues of the validity of the available secondary information due to problems such as bias in the data set, which potentially can emerge from either political or commercial motivations. From my own reading of secondary information on identity fraud, reports from companies such as Unisys (2009) and McAfee (Paget, 2007) are regularly quoted in the media. However, companies such as these benefit commercially by winning contracts and selling ‘fix-it’ products, as a result of the apparent increasing prevalence of identity fraud. Therefore, additional validation is warranted against other sources of similar (if not the same) information and/or statistics.

It is important to note that comparing and evaluating secondary information for validation purposes is not a clear cut process because we “cannot assume that available data are accurate, even when they appear to measure the concept in which we are interested in a way that is consistent across communities” (Schutt, 2006, p. 103). Additionally, Stewart (1984) states, “Noncomparability of data is a serious problem when one is making comparisons across information from multiple sources. National Governments often differ in both the methods employed to collect data and the definition of categories” (p. 44). In identity fraud, secondary data consistency problems can include differing classes of offences between agencies, an interchangeable use of terms such as ‘false’, ‘fraudulent’ and ‘counterfeit’, different

reasons for recording data and differing levels in the amount of data required. Moreover, agency opinion varies on what constitutes an offence. In relation to governmental secondary sources, Gomm (2004) states that, "Such data are primarily used for internal agency purposes and for the external monitoring of their performance. They are a product of the way such services are organised" (p. 140). In New Zealand, Gomm's comment would mean that secondary data and information are published in line with governmental outcomes. However, governmental outcomes are a reality that justifies budget allocations to agencies. The fact that they are politically driven does not make the secondary sources any less valid, unless of course, the data was purposely manipulated. Stewart argues that "government agencies are frequently prone to find answers to questions, no matter how unrealistic, rather than admit to not knowing" (p. 59). Unfortunately, in my own experience, I have known this to be true in one case, albeit not in a research capacity.

The issues surrounding the reliability and validity of secondary information are compounded when secondary information originates in an overseas country. Stewart (1984) cautions, "Another problem with secondary data in other nations is a lack of reliability. Official statistics often reflect national pride and international political considerations rather than reality" (p. 43). New Zealand ranks first equal with Finland and Iceland on the Transparency International's *Corruptions Perceptions Index 2006* – an international survey which measures the perceived bureaucratic corruption in each country in the world. Less transparent states may be prepared to publish erroneous statistics to satisfy not only their own agenda, but also to quiet international organisations and any pressure from other countries to perform on the world stage. Consideration must also be given to the fact that what is classified as an offence in one country, may not be an offence in another. Moreover, due to the borderless nature of

identity fraud, diplomatic and agency issues often effect any formal judicial processes and hence, subsequent quantitative recording. There is also the possibility that one identity crime can be recorded in two or more countries by two or more agencies, as the following example demonstrates:

If an Iranian on a false German passport departs from Frankfurt and travels to Beijing and Kuala Lumpur en route to New Zealand, and is stopped by the New Zealand Airline Liaison Officer in Kuala Lumpur, who identifies that he has a false German passport, there are a number of operative issues in recording this false document and the associated identity crime. It is possible that the Iranian pays a bribe to Malaysian Immigration and is released without charge – therefore no identity crime is recorded in Malaysia. It is possible that the New Zealand Liaison Officer will record the identity crime with Immigration New Zealand as the Iranian was en route to New Zealand. It is possible that the Malaysians will charge the Iranian in which case both the Malaysian Police and Malaysian Immigration will hold records of the identity crime. It is possible that the Malaysians will return the Iranian to the last country that he was landed under Annex 9 of the *ICAO Convention*. This could be China or Germany. Therefore, more than one agency in both of these countries could both record the one identity crime (Immigration, Police, Foreign Affairs, Passport Office). Moreover, Germany could also record the identity crime even if the Iranian is not sent back there because he had a false German passport. If Malaysia is able to return the Iranian to Iran, the Iranian Government also may record the same identity crime. This example illustrates that quantitative recording of identity fraud is not a straightforward process and, that questions of reliability and validity effect whether the available data are a true representation of all identity crimes being committed. Gomm (2004) describes the difficulty of multi-agency reporting of secondary data by stating:

They are often produced in a haphazard way with contributions by many different agencies classifying events and people differently, and rarely in ways that are consistent through time. Unlike well-constructed research there are rarely any clear protocols for recording, rarely any checks on the reliability of recording and little to control the effects of bias on the recording process. (p. 148)

While identity fraud is not a new crime, the world has taken notice since the terrorist attacks in New York on September 11, 2001. An increase in attention has brought an increase in recording of secondary information in the field, but in a historical sense there is not a lot of comparable or historical information available. The increase in recording in this short period since 2001 can also be attributed to the wide sweeping legislative changes in the western world to accommodate identity related offences. However, swift legislative changes can mean an action is legal one year and illegal the next year. This also impacts upon statistical reporting. In this vein, Gomm (2004) advises that “sometimes researchers have little choice but to utilise data which are generated by the routine operation of bureaucratic agencies” (p. 140). In New Zealand, research is sometimes limited to quantitative statistics published by agencies that have sole charge for certain state functions. Examples of these include Land Transport New Zealand who administer the driver licence database; Department of Internal Affairs who administer births, deaths and marriages register, as well as the passport database. Therefore, secondary sources in my research are somewhat limited. Schutt (2006) states that, “It is only after factors such as legal standards, enforcement practices, and measurement procedures have been taken into account that comparisons among communities become credible” (p. 103). However, doing this exercise in itself would take a substantial amount of time and research.

In fact most commentators agree that secondary data needs to be re-evaluated as Hinde (2002) states: “You may have to transform and manipulate the data in quite

complex ways to render them suitable for testing the hypothesis you wish to test” (p. 253) and as Kelsey (2001) states: “Using secondary sources means the researcher needs to work extra hard at ensuring that the data in those existing reports are both valid and reliable” (p. 309). In theory this is obviously a preferential process. But in reality, the secondary *data* is not always available and the researcher must rely on published secondary *information* only. Moreover, re-evaluating someone else’s data defeats the advantages of secondary sources, namely “the considerable savings in time and cost to be made by obtaining your data directly” (Hinde, p. 251). Having to research the basis of someone else’s data and gain comprehension from it is a labour intensive task per se – especially if a large number of secondary sources are being utilised. It raises the question of whether it would be easier and thus more cost-effective, to do the research yourself from the start. In contrast to some other commentators, Hinde actually states, “Many secondary data sets are of high quality, having been produced by experts in the arts of questionnaire design and fieldwork” (p. 251). Moreover, political or commercial bias would be difficult to prove in evaluating any secondary data. In support of governmental sources, Schutt (2006) advises that “government reports are rich and readily accessible sources of social science data” (p. 102). Thus, while caution must be taken of glaringly obvious signs of bias in secondary sources, “Secondary analysis, by definition, builds on previous work, and so fits naturally within the process by which new knowledge is created” (Dale, Arber & Procter as cited in Hinde, p. 252).

3.5 REFLEXIVITY

In my thesis, evidence of reflexivity is dispersed throughout – this is a reflexive comment in itself. Finlay (2003) states: “Reflexivity in qualitative research – where

researchers turn a critical gaze towards themselves – has a history spanning at least a century” (p. 3). Before I explain further regarding the use of reflexivity in relation to this thesis, I will begin by examining the definitions of *reflexivity*, which tend to vary according to the context in which reflexivity is placed. In a sociology context, *“‘reflexivity’ is the regular exercise of the mental ability, shared by all normal people, to consider themselves in relation to their (social) contexts and vice versa”* (Archer, 2007, p. 4). More specific to my research, reflexivity in a research context has been described insofar as: “that researchers adopt a third-party viewpoint on their own research activities: they treat themselves, as it were, as research subjects in their own research” (Gomm, 2004, p. 240); “Reflexivity is the process through which a researcher recognizes, examines, and understands how his or her own social background and assumptions can intervene in the research process” (Hesse-Biber & Leavy, 2006, p. 146).

In this vein, it is both my employment background and my social background that influence my beliefs and may impact upon this research into identity fraud. Socially, I come from a white, middle-class existence and the way I was brought up influences my view of the world, including my conceptualisation of what is right and wrong. In my view, committing an identity crime is wrong whereas, had I been brought up in a rural Indian village where survival is life’s prime objective, then my view may be entirely different. Furthermore, my employment history has also influenced the way in which I view identity fraud, largely due to working in a compliance capacity with the New Zealand Government. However, at the same time, by interacting with people who have committed identity fraud, I have had the opportunity to listen to their stories and gain insight into ‘their world’. Therefore, my view has been somewhat balanced. Maso (2003) states:

Subjectivity is an inevitable part of the research process Researchers bring with them their own emotions, intuitions, experiences, meanings, values, commitments, presuppositions, prejudices, and personal agendas, their position as researchers and their spontaneous or unconscious reactions to subjects and events in the field. (p. 40)

It is thus imperative that bias be minimised in this research.

Bias introduced into any research process affects the validity and reliability of the research and “reflexivity is the way that qualitative researchers strive for reliability and validity” (Delamont, 2004, p. 226). By openly commenting throughout the research process on my own thoughts and opinions, I am creating a transparent narrative in which the reader is able to understand my arguments within a contextual framework. For example, if I were to comment that many forged and counterfeit passports are purchased on the streets of Bangkok without stating my justification for this comment (that is, because I have had many asylum seekers arriving at the airport telling me this among other things), then the reader would not treat my comment as being valid. A lack of validity, in turn, impacts upon the reliability of this information. Maso (2003) reinforced the validity argument by stating:

While subjectivity has acquired something of a bad name because of the ‘scientific’ demands of validity and reliability, researchers realise that the practice of research makes an element of subjectivity inescapable. This is why inquirers, through the use of reflexivity, are required to ‘come clean’ about how subjective and intersubjective elements have impinged on the research process in order to increase the integrity and trustworthiness of their research. (pp. 40-41)

Therefore, the use of reflexivity also crosses into the ethical arena in this research and is applicable in disclosing such ethical issues as research sponsorship and confidentiality matters. I have captured my reflexive thoughts on the research process through the use of a journal, which enables timely and accurate entries to be recorded.

As I commented at the beginning of this section, reflexivity has manifested itself throughout this thesis. I have done this through the use of both real-life examples and by posing hypothetical realities. This technique allows the reader to regularly understand my standpoint as well as providing a high level of transparency to my own thoughts on the subject at hand. Gough (2003) supports this demonstration of reflexivity by stating:

One technique is to disrupt the narrative flow of the text with commentaries at the end of each section, thereby counter-posing the academic analysis with more personal (e.g. identifying researcher emotions) reporting (Lather, 1992). In this way, the dual positions of the researcher become apparent ... (Seale, 1999). (p. 30).

Moreover, a continuous use of reflexivity adds depth to the research, by allowing the reader a glimpse of a world that they have not seen themselves. Conversely, the use of reflexivity has forced me, the researcher, to practically apply academic theories and principles to my real-life experience. To my surprise, I have found that the two do not always correlate, but this discovery per se is poignant. Alvesson and Sköldbberg (2000) concur by commenting: “The whole idea of reflexivity, as we see it, is the very ability to break away from a frame of reference and to look at what it is *not* capable of saying” (p. 246).

Reflexivity is an important practise, not just for the researcher but also for the research participants. I noted from interviewing my key informants that they sometimes felt pressured into answering my questions on the spot, and appeared mindful not to keep me waiting too long for their responses. Part of my research process involved sending the written transcripts of my interviews to my key informants, not just for the purpose of correcting any errors, but for the purpose of adding to their responses in their own time. Savin-Baden (2004) stated:

Helping participants to become reflexive means not just returning the transcripts for validation but constructing the data interpretatively and asking for them to examine not just the construction but also where they feel they are in relation to the interpretations. (p. 371)

Nonetheless, Finlay (2003) warned:

Reflexivity is not without its critics or its pitfalls. In offering a methodological account, researchers seeking to promote the integrity of the research need to grapple with the problematic spectre of having a single, 'true' account. Does the process of explicitly situating the researcher invariably produce a better account or might it function as an unwitting strategy to claim more authority? (p. 17)

As previously stated, subjectivity is inherently present in research and it was therefore an appropriate aim to minimise the risk. In my research, I actively strove for objectivity and more than a "single, 'true' account" through the use of triangulation in my methods. Where possible, the use of secondary sources and key informants gave authority to my own opinions and participant observation. Conversely, Hesse-Biber and Leavy (2006) advocated the use of 'difference' in the research process and stated:

Reflexivity also reminds us that we need to be mindful of the importance of difference to our research as a whole. Difference enters into the projects we select, the questions we ask, the way data is collected, analyzed, written and interpreted. Difference needs to be explored, not disavowed. (p. 141)

My opinion is what makes the difference between my thesis and the next person's thesis and it promotes growth in the research field. If we all had the same experience and the same opinions, research and knowledge would evolve at a much slower pace. Finlay (2003) comments: "The challenge for researchers using introspection is to use personal revelation not as an end in itself but as a springboard for interpretations and more general insight" (p. 8). The world is made up of human beings with opinions but it is how these opinions are harnessed that makes them useful in building research and knowledge capabilities. In the identity fraud field in New Zealand, there is a large research gap and reflexivity in this thesis will assist in filling that gap, by providing real

life examples combined with the authoritative voice of key informants and secondary information.

4 LITERATURE REVIEW

Literature in the identity fraud field has escalated in recent times, particularly since the 9/11 terrorist attacks in 2001, where it was discovered that the terrorists had obtained false identities in order to board and hijack aircraft in the attack on the World Trade Center in New York. The aftermath of 9/11 saw the United States Government reassess its national security, intelligence and immigration policies and *The 9/11 Commission Report* publicly stated:

In the decade before September 11, 2001, border security – encompassing travel, entry, and immigration – was not seen as a national security matter In national security circles, however, only smuggling of weapons of mass destruction carried weight, not the entry of terrorists who might use such weapons or the presence of associated foreign-born terrorists.

For terrorists, travel documents are as important as weapons. Terrorists must travel clandestinely to meet, train, plan, case targets, and gain access to attack. To them, international travel presents great danger, because they must surface to pass through regulated channels, present themselves to border security officials, or attempt to circumvent inspection points.

In their travels, terrorists use evasive methods, such as altered and counterfeit passports and visas, specific travel methods and routes, liaisons with corrupt government officials, human smuggling networks, supportive travel agencies, and immigration and identity fraud. (2004, pp. 383-384)

Another reason for the increase in identity fraud literature can be attributed to the increase in the use of biometrics in identity documents such as passports in the Western world and the increase in online activity. Nonetheless, comparative to other related subject areas such as financial crime, *specific* literature on identity fraud is scarce, particularly in the academic arena and even more so in New Zealand. Anderson, Durbin and Salinger (2008) remarked that “both the theoretical and empirical literatures on identity theft are in their infancy” (p. 172). In respect of

resolutions to identity fraud, identity management has now come to the fore. Hosein (2008) stated:

The field of identity management has changed dramatically in just a few years Five years ago we were begging for some attention from our governments, industries, and consumer protection institutions. Now, everyone seems to be in agreement that something must be done about identity management. (p. 3)

However, finding comprehensive, effective, efficient and acceptable identity policies and management systems is far from being resolved. While the private sector holds a vested interest in protecting itself from identity fraud, *official* identity data is held by governments around the world. Governments attempting to develop solutions and public policy relating to identity fraud are fraught with both international and domestic political issues.

In this section, the concept of identity fraud is examined as the definition per se has varying definitions in the literature and between countries. Secondly, identity fraud in New Zealand is discussed, followed by an examination of some of the issues in systems in New Zealand. Lastly, both the policy and legislation in relation to identity fraud in New Zealand are investigated. The literature in identity fraud is largely dominated by government and industry reports as well as media articles. For the purpose of this thesis, the literature examined was that which was published prior to 30 June 2009.

4.1 CONCEPTUALISING IDENTITY FRAUD

Before the term identity fraud is discussed, it is important to understand the concept of identity as referred to in this thesis. Raab (2008) discussed the issues surrounding the conceptualisation of identity:

‘Identity’ and ‘identification’ are among the most elusive and difficult concepts confronting scholars and researchers in the broad field of information studies, reflecting a welter of discourse in many other fields,

including philosophy, psychology and sociology But identity and identification are not just specialist terms used only by researchers in our various technical discourses. They feature predominantly in casual everyday use by our citizens, politicians, legislators, the media, public and private organisations, and many more domains as well The enormous and diverse literature that surrounds the term 'identity' testifies to the growing importance of identity in the politics and social life of our time. (p. 4)

Opinion is varied between commentators. In examining 'identity' from a psychological standpoint, McAdams, Josselson, and Lieblich (2006) stated that "identities are not fixed and frozen" as individuals evolve in time (p. 7), yet Raab (2008) stated: "A fixed identity may be necessary if we are to function in daily life, and history attests to the severe difficulties that befall persons whose 'papers' have been destroyed or confiscated, and who therefore need to construct an identity" (p. 7). Therefore, the context in which one refers to identity, greatly affects the concept of identity. Identity theory, while sounding relevant to this paper, is not specific to identity fraud and has been defined as follows: "Identity is a set of meanings applied to the self in a social role or situation, defining what it means to be who one is in that role or situation" (Cast, 2003, p. 43). How an individual identifies oneself is relevant to identity in a generic context but Koops, Leenes, Meints, van der Meulen, and Jaquet-Chifelle (2009) distinguish identity between "*Idem* identity, that is, the sameness of things or persons, and *ipse* identity, that is, personal identity in the meaning of an individual's sense of self" (p. 3). In the discussion surrounding identity fraud in this thesis, it is 'idem' identity that will be the concept utilised, as this is relevant to identity fraud being committed by individuals, against what Goffman (1990) termed *identity pegs* (p. 73). Identity pegs are factors that make an individual unique:

The whole point of these various identification devices is, of course, that they allow no innocent error or ambiguity, transforming what would be merely a questionable use of socially informing symbols into clear-cut

forgery or illegal possession. Therefore the term identity document might be more accurate than identity symbols. (p. 78)

The definition around the term *fraud* is much more straight-forward. Smith (2008) defined fraud simply as “crimes involving dishonesty, collectively known as fraud” (p. 379). The Organisation for Economic Co-operation and Development (OECD, 2009) provides a more detailed explanation:

According the UN IEG⁵, the element of deception, and hence the term “fraud,” lies not in the use of deception to obtain the information, but in the subsequent use of the information to deceive others. As with economic fraud, this element of deception includes the deception of technical systems as well as human beings. (p. 49)

The UN IEG definition is somewhat at odds with New Zealand legislative provisions. Section 228 (Dishonestly Taking or Using Document) of the *Crimes Act 1961* recognises the taking or obtaining of information on fraudulent grounds as an offence. However, the *Crimes Act 1961* does not provide any interpretation or definition for the term “fraud”.

Once combined, *identity fraud* is not as simplistic a term as what I first believed at the outset of this thesis. For the purpose of this thesis, I defined identity fraud operationally as: the deceptive use of a fictitious or another person’s identity to commit civil or criminal offences for a benefit or advantage. Nonetheless, definitions in the identity fraud field are not currently standardised, with American literature adopting the term *identity theft* for those offences that would often fall under the term identity fraud in other countries. Koops et al. (2009) advised of the challenges in defining identity-related terminology:

It is also not clear what exactly constitutes ‘identity theft’ or ‘identity fraud’ and how these can be combated ... This lack of precision becomes especially apparent when comparing the various official media reports on

⁵ UN IEG is an acronym for United Nations Intergovernmental Expert Group.

these topics. Definitions are hardly ever provided, even though the statistics play a role in politically motivated discussions and policy decisions. Commonly accepted definitions are also lacking in literature. This means that we are at the stage where comparisons of apples and oranges abound making it virtually impossible to determine the real incidence of identity-related crimes. (p. 2)

In New Zealand, where identity fraud statistics are lacking, this poses significant problems for any future work in this area and has subsequent implications for public policy and legislative provisions, especially in the classification of offences (see Secondary Information). In an attempt to create consistency in the use of terminology, The Australasian Centre for Policing Research (2006) developed the following definitions for three commonly used terms:

Identity crime refers to offences in which a perpetrator uses a false identity in order to facilitate the commission of a crime. (p. 9)

Identity fraud refers to the gaining of money, goods, services or other benefits through the use of a false identity. (p. 9)

Identity theft involves the theft of a pre-existing identity. (p. 10)

Nonetheless, “It needs to be recognised that the term ‘identity crime’ is used fairly loosely. A number of State, Territory and Commonwealth agencies appear to use the terms ‘identity crime’ and ‘identity fraud’ interchangeably” (Australasian Centre for Policing Research, p. 5). The OECD (2009) reports that identity theft is a subset of identity fraud and that both identity fraud and identity theft are a subset of identity crime (p. 49).

4.2 THE NEW ZEALAND IDENTITY FRAUD ENVIRONMENT

It is common to hear in the media that incidences of identity fraud are on the increase. Identity fraud is an enabler of other crimes and it facilitates organised crime. The *Organised Crime Strategy 2008-2009* (New Zealand Ministry of Justice, 2009) states:

International organised crime is estimated to be worth US\$2 trillion and in New Zealand, enforcement agencies consider organised crime as growing, as it is offshore Identity fraud is an integral part of organised criminal offending. The Department of Internal Affairs detected 105 fraudulent passport applications between 2002 and 2006. (p. 4)

In addition, a global rise in the usage of online services such as banking, has paved the way for new methods in identity fraud to emerge, such as phishing⁶. However, New Zealand's lack of statistics and classification of offending does not capture identity fraud as it is occurring in New Zealand.

New Zealand Government collated statistics on identity fraud are scarce. The New Zealand Police administer a database of misused identities, collected from other New Zealand agencies. However, there is a reliance on employees in those agencies to refer their cases to the Police. Many agency employees are too busy to send their referrals through and it is on a voluntary basis that the information is provided. The benefits to other Government agencies from having access to such a database are enormous, as long as it is utilised. New Zealand appears more advanced than the United States in this regard, however, with Gordon and Willox (2006) reporting that in the United States "little progress has been made in developing a national database of identity fraud incidents. UCR⁷ and NIBRS⁸ do not include a category to collect this information" (p. 3). New Zealand's relatively small size as a nation and centralised government enables the collection of such data vis à vis the United States or Australia which have both federal and state levels of government to contend with. Multiple levels of government create further difficulties in the co-ordination and collection of identity fraud data.

⁶ Anderson et al (2008, p. 172) define *phishing* as "a form of spam that tries to entice the recipient to send along the information needed to steal an identity". This spam is sent to email users.

⁷ UCR is an acronym for Uniform Crime Reports. They are administered by the FBI in the United States.

⁸ NIBRS is an acronym for National Incident-Based Reporting System.

In one of the few surveys relating to identity fraud in New Zealand, the KPMG Forensic Fraud Survey 2008 of Australian and New Zealand companies stated that:

- 3% of fraud committed by managers was identity fraud in 2006. There was no figure in 2008 (p. 9);
- 7% of frauds were lending fraud (identity fraud), committed by external parties in 2006 in the financial services sector. This figure reduced to 2% in 2008 (p. 13);
- 1% of frauds were identity fraud, committed by external parties in 2006 in the non-financial services sector. There was no figure in 2008 (p. 14);
- Identity fraud was listed in a category of “identity fraud and other related fraud” when listing the major fraud types. There were three frauds in total in this category, totalling \$1,231,207, with the average fraud representing \$410,402 (p. 16);
- 15% of the largest fraud cases involved an element of identity fraud (p. 34);
- The most common fraud involving identity fraud was credit card fraud. These totalled 154,602 cases, totalling more than \$90 million (p. 34);
- In relation to the statement: “My organisation takes active steps to educate its customers about identity fraud and the steps to take if they believe they are a victim”, 24% of respondents agreed with this statement and 39% disagreed (p. 34);
- In relation to the statement: “My organisation has appropriate customer identification procedures”, 67% of respondents agreed with this statement and 16% disagreed (p. 34);

- In relation to the statement: “My organisation has taken appropriate steps to ensure the identity of all third party service providers contracted to perform work for my organisation”, 57% of respondents agreed with this statement and 26% disagreed (p. 34); and
- In relation to the statement: “My organisation has taken appropriate steps to ensure the identity of all employees commencing employment”, 79% of respondents agreed with this statement and 12% disagreed (p. 34).

Despite the collation of the above statistics by KPMG, in my experience the following factors may have impacted on the results of their Fraud Survey:

- Financial institutions do not want to harm their reputation by reporting all instances of identity fraud.
- The classification of offending may skew results, in that financial institutions are more likely to record any fraud under a financial category, such as mortgage fraud or credit card fraud, rather than separately report identity fraud.
- The legislative provisions in one’s respective jurisdiction will often dictate the way in which fraud incidences are recorded, for instance, if there is no specific identity fraud legislation then it is unlikely to be recorded as an offence per se.
- Products issued by financial institutions may have been abused in jurisdictions outside of their control, for example, credit card data could be purposely given or stolen online and/or overseas. These incidences may not have been reported and/or prosecuted.

- There is often a time lag between the offence date and the date of detection of the identity fraud, thus more offences may have taken place in 2008 that have not yet been discovered.
- It is unknown as to whether the reported statistics on identity fraud were for confirmed/prosecuted cases or merely suspected cases of identity fraud.

The April 2009 *New Zealand Consumer Link Survey* by Unisys Security Index stated that the top three areas that New Zealanders were concerned about were as follows:

Other people obtaining credit card/debit card details

Unauthorised access to or misuse of personal information

Computer security in relation to viruses or unsolicited emails

All three of these areas carry risk in terms of enabling identity fraud to occur. Unisys added that they had “released additional research which shows that the majority of New Zealanders believe that the risk of identity theft will increase as a result of the global economic crisis” (p. 3). More specifically, the Unisys survey revealed that:

- 58% of New Zealanders or an estimated 1.8 million people are very or extremely concerned about someone else obtaining their credit/debit card details. This was an increase of 7% (or approximately 220,000 people) since September 2006 (p. 5);
- 46% of New Zealanders or an estimated 1.5 million people are very or extremely concerned about their computer security. This was an increase of 9% (or approximately 290,000 people) since September 2006 (p. 6);
- 37% of New Zealanders or an estimated 1.2 million people are very or extremely concerned about conducting banking or shopping online. This was an

increase of 8% (or approximately 260,000 people) since September 2006 (p. 6);


and

- 58% of New Zealanders or an estimated 1.8 million people are very or extremely concerned about unauthorised access to or misuse of their personal information. This was an increase of 9% (or approximately 290,000 people) since September 2006 (p. 7).

In general, the New Zealand Customs Service (NZCS, 2009) summarised the current criminal climate in which identity fraud breeds:

Trans-national organised criminal syndicates operate internationally without boundaries. Criminal activity is more sophisticated, and technology is changing rapidly The global economic downturn is taking effect in New Zealand. Consequently, Customs expects to see a rise in illegal activities, represented by more smuggling, fraud. (p. 15)

The fact that criminals are targeting New Zealand was evidenced through the establishment of a website in May 2009, purporting to be the Massey University Students' Association (MUSA). This website advertised 'fake passports' and driver's licences for sale for countries such as Australia, the United States, Germany, Mexico, France, Belgium. It has now been shut down but Figure 4 (next page) is a scanned copy of part of the page:



MUSA
Massey University Students' Association

[FAQ](#) [Search](#) [Memberlist](#) [Usergroups](#) [Register](#)
[Profile](#) [Log in to check your private messages](#) [Log in](#)

Search found 30 matches

MUSA Forum Index




Author	Message
<p> Topic: BUY AUSTRALIAN FAKE PASSPORT,FAKE PASSPORT OF AUSTRALIA FOR</p> <p>SellingPassports</p> <p>Replies: 0 Views: 11</p>	<p> Forum: <u>Rantings</u> Posted: Tue May 12, 2009 6:28 am Subject: <u>BUY AUSTRALIAN FAKE PASSPORT,FAKE PASSPORT OF AUSTRALIA FOR</u></p> <p>Our team is a unique producer of quality fake documents. We offer only original high-quality fake passports, driver's licenses, stamps and other products for following countries: USA, Australia, B ...</p>
<p> Topic: BUY FAKE MEXICAN PASSPORT,FAKE PASSPORT OF MEXICO FOR SELL</p> <p>SellingPassports</p> <p>Replies: 0 Views: 10</p>	<p> Forum: <u>International Students</u> Posted: Tue May 12, 2009 6:27 am Subject: <u>BUY FAKE MEXICAN PASSPORT,FAKE PASSPORT OF MEXICO FOR SELL</u></p> <p>Our team is a unique producer of quality fake documents. We offer only original high-quality fake passports, driver's licenses, stamps and other products for following countries: USA, Australia, B ...</p>

Figure 4: Fake Massey University Students' Association Webpage

Another website, FakeID (n.d.), advertises 'fake' identity documents such as passports, driver licences, identity cards and stamps (port stamps for arrivals and departures as used in an airport). Some of the images of fake passports and driver licences on offer are contained on their website (see Figure 5):

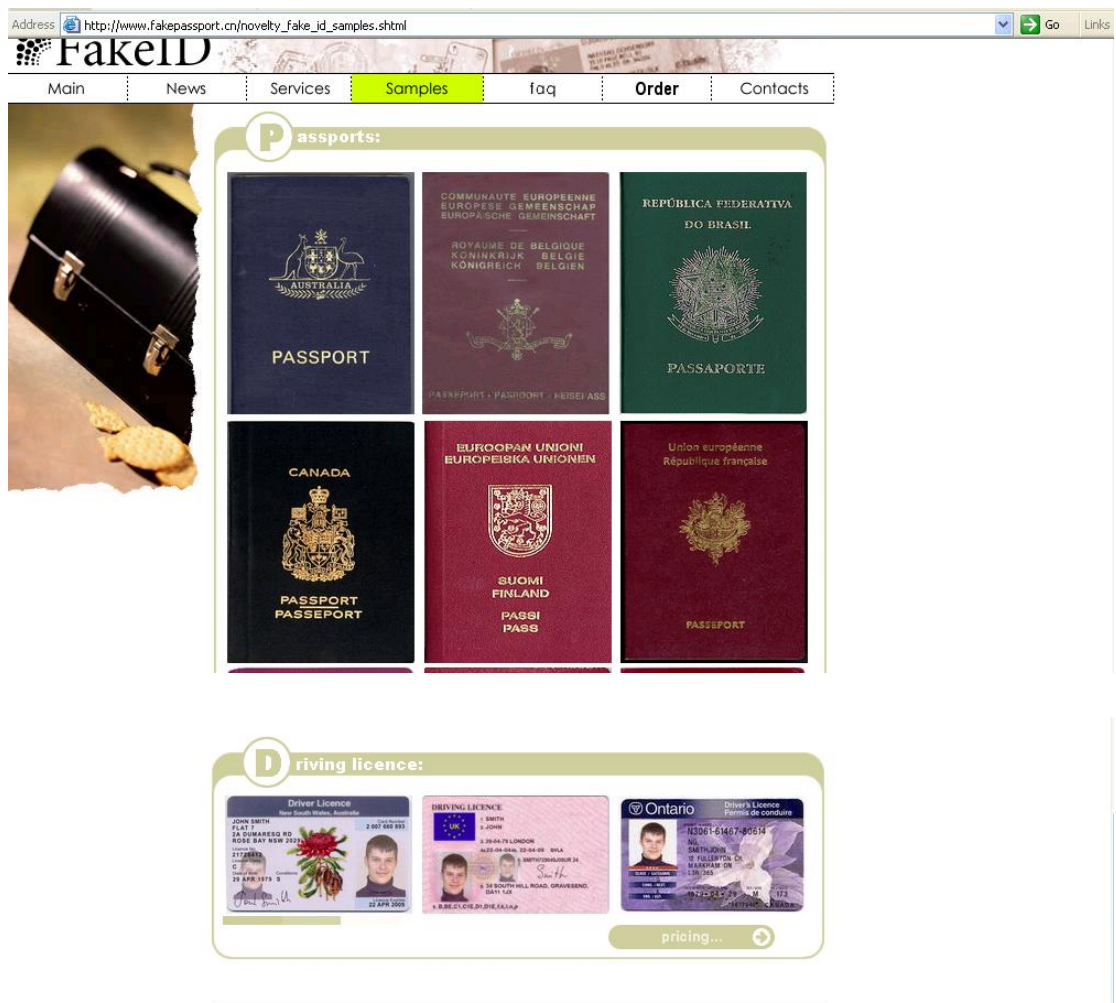


Figure 5: Website - Fakepassport.cn

Other unsuspecting online users place scanned pictures of their identity documents at www.photobucket.com which is a website that provides shareware for the downloading of photos. It is common to see scanned images of individual's passports, complete with their photos and bio data for the world to see. Below (Figure 6) is an image of a Filipino passport and a national identity card.

Address <http://media.photobucket.com/image/passport/gladicemae/passport.jpg?o=75>

visit to see this lucky banner.

help | login [Join Now](#)

photobucket | [join now](#) | [find stuff](#) | [what's new](#) | [images](#) | [Search](#) powered by Ask

top categories | icons | photography | quotes & sayings | art | funny | popular videos | group albums | contests

Viewing 75 of 6,605 (More Results)

Related videos (93) | More from user (2)

Live and work in the US

Name:
 Email:
 Telephone:

TRY IT NOW

© DINK MEDIA GROUP

▼ Share this image

See more passport pictures | [Follow](#)

By [gladicemae](#) Views: 13 Rate: ★★★★★ 0 ratings

photobucket | [join now](#) | [group albums](#) | [find stuff](#) | [what's new](#) | [images](#) | [Search](#) powered by Ask

top categories | icons | photography | quotes & sayings | art | funny | popular videos

Viewing 1 of 5 (More Results)

You're at the beginning

More from user (970)

Congratulations!

We think **your IQ** is higher than **85% of the population!**
[Click on OK](#) to find out if we are right!

See more national identity card pictures | [Subscribe](#)

By [aartt](#) Views: 7 Rate: ★★★★★ 0 ratings

Subas Chandra Bose's INA. "AZAD HIND FAUZI" IDENTITY CARD

Figure 6: Website – Photobucket.com

These incidences are not limited to foreign nationals. A Google search of images of New Zealand documents revealed a New Zealand driver licence and a student card from the University of Otago (see Figure 7 below). While some pertinent details have been blurred on the driver licence, locating this person through other means is not difficult based upon the information that he has revealed. The University of Otago student card not only identifies the student with his photo, but also reveals his username and email address. In both cases, there is sufficient personal information

combined with the holder's photo image for this information to be used in fraudulent activity.

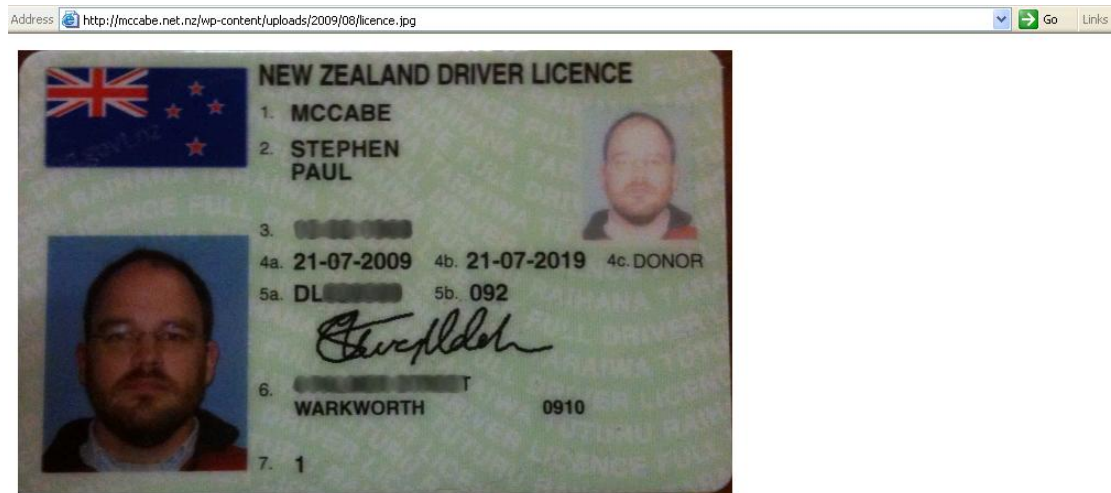
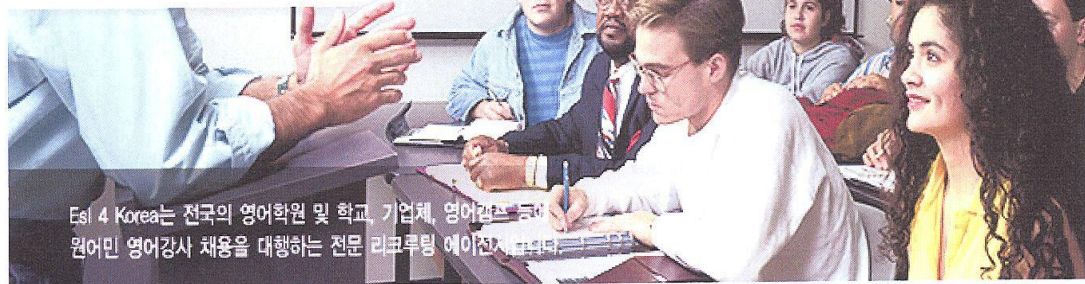


Figure 7: New Zealand Identity Documents Displayed from a Google Image Search

One of the most alarming displays of identity came in the form of a New Zealander, whose New Zealand passport bio data page had been published on a Korean ESL webpage (see Figure 8 on the following page). Ms McIlroy, in combination with her passport image had listed a personal profile. Information on this profile such as her marital status, her educational degrees and associated major, her date of birth, her



ESL 4 Korea는 전국의 영어학원 및 학교, 기업체, 영어캠프 등에
 원어민 영어강사 채용을 대행하는 전문 리크루팅 에이전시입니다.

E4K QUICK MENU

ESL 4 Korea

강사 자격

채용조건

채용절차

CLICK
원어민강사 채용신청

E2VISA

출입국관리소

초청필요서류

서류양식 다운로드

좋은강사를 구하는 요령

전입 및 외국인 등록

FAQ

Information

상담/문의

02-364-0591

02-364-0595

02-785-0596

24시간 연중무휴 상담가능

E-mail :

master@esl4korea.com

◎ 추천 원어민 강사 (Full time)

Home > 외국인/교포

Sonya Jane McIlroy



<input checked="" type="checkbox"/> No	107
<input checked="" type="checkbox"/> Name	Sonya Jane McIlroy
<input checked="" type="checkbox"/> Gender	Female
<input checked="" type="checkbox"/> Nationality	New Zealand
<input checked="" type="checkbox"/> Starting Date	2005-4-1
<input checked="" type="checkbox"/> Desired Location	Big City
<input checked="" type="checkbox"/> Birth Date	1975-10-23
<input checked="" type="checkbox"/> Marital Status	Single
<input checked="" type="checkbox"/> Desired Teaching Level	Not specified
<input checked="" type="checkbox"/> Saturday Work	Not specified
<input checked="" type="checkbox"/> Degree you have	4-Year BA/BS
<input checked="" type="checkbox"/> Major	Linguistics Major
<input checked="" type="checkbox"/> Minor	
<input checked="" type="checkbox"/> Teaching certificate	
<input checked="" type="checkbox"/> Desired Pay Per Month	Not specified
<input checked="" type="checkbox"/> Desired Housing	Single Housing

Figure 8: New Zealand Passport Image and Personal Information Displayed Online

name, her desired housing, her starting date and her reference number is all information of extreme value to an identity fraudster or other organised criminal group. This webpage publicly details information about her personal life that a stranger would not otherwise know. It contains more than enough information for an individual to potentially manufacture forged or counterfeit documents in her identity and subsequently assume her identity.

At a strategic level, the New Zealand Office of the Auditor-General's report (2007) into the management of identity fraud in the Department of Labour (DOL), specifically INZ, identified the problematic spread of identity fraud as follows:

Identity fraud has been recognised as one of the most pervasive developments in fraud in recent years. The Department⁹ has recognised that, with a proliferation of the narcotics trade, many organised criminal groups use false travel documents and falsely-obtained immigration status to aid their offending Improvements in document forgery and an increase in identity theft have also led to more opportunities for individuals or organised groups to circumvent New Zealand's border controls. The Department has identified an increasing number of cases of individuals lodging multiple refugee claims under different identities, and cases of people previously removed from New Zealand who return under false identities. (p. 19)

Identity fraud facilitates illegal migration also for people other than refugee claimants. Interpol (2008a) cites the use of false travel documents by organised crime groups as an enabler of the trafficking in human beings, such as women trafficked from their home country to a foreign country for sexual exploitation (p. 1). From my own experience I can say that this does occur in New Zealand. In addition, people smuggling (usually of economic driven migrants) is facilitated by identity fraud and also regularly occurs in New Zealand. The following statement from Interpol (2008b) reveals the people smuggling process:

⁹ "The Department" refers to the Department of Labour.

The modus operandi of criminal organizations is increasingly sophisticated, with numerous affiliated crimes linked to people smuggling, such as identity-related crimes, corruption, money laundering and violence (including debt bondage and murder). For organized crime groups, smuggling humans across borders is a low-risk, high-profit business. People can be smuggled by air, sea or land, often by complex routes which can change rapidly if detected by law enforcement officers. The welfare of the migrants is rarely a consideration; they are frequently subjected to inhumane conditions, and thousands die annually en route to their destinations. (p. 1)

Interpol's statement above raises a number of issues to be faced by governments worldwide, including the New Zealand Government. Such issues include enforcing the law across multiple jurisdictions including international borders; balancing the risk at the border versus the facilitation of passengers; adhering to international obligations relating to people smuggling and human trafficking; managing the multiple number of agencies that may have an interest in an individual who has been smuggled and the people smuggling ring of which he or she may have been a part; allocating Government resources to this problem. These issues and governmental responses all form a part of the identity fraud system. The issues in New Zealand are further outlined in the next section.

4.3 IDENTITY FRAUD SYSTEM ISSUES

The Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General in Australia outlined four ways in which identity fraud can occur, in their March 2008 report entitled *Final Report Identity Crime*. The four methods were:

1. **Online Techniques – general:** "Identity-related criminal activity is constantly evolving as new ways to gain access or to manipulate identity data are found" (p. 5). Techniques include phishing in order to gain an individual's bank details.
2. **Online Social Interaction:** "Online social interaction, particularly social networking, is growing in popularity, However, some users of social networking

websites engage in behaviour that puts them at risk of identity theft” (p. 6).

Social networking sites include Facebook, My Space and Bebo. Some individuals place important personal data on their social pages including email addresses, mobile phone numbers and general personal information about themselves.

3. **Consumer Scams:** The infamous Nigerian scams fall under this category.

Consumer scams often advise an individual that they have won a lottery, have inherited money from an unknown relative overseas, for example. The scammers then request that the individual supply them with their personal details, often requesting a copy of their passport and their credit card or bank account details. When this information is supplied, their identity can be stolen, their bank accounts emptied and their credit card is used unlawfully for purchases. The Australasian Consumer Force Taskforce was established in 2005 to tackle the problem of consumer scams. “It comprises all the governmental regulatory agencies and departments in Australia and New Zealand that have responsibilities for consumer protection” (p. 7).

4. **Traditional Techniques:** “Dumpster diving” – examining an individual’s rubbish in search for personal documents such as bank statements. These can assist in gaining identity details. “Shoulder surfing” – standing behind an individual as they enter a PIN number for example (p. 7).

Consumer concerns detailed in the 2009 *New Zealand Consumer Link Survey* relating to identity fraud in New Zealand are in line with research conducted by Deloitte in their 2006 Global Security Survey. Deloitte stated that identity theft is “the crime of the 21st Century” (p. 13) and consequently, financial institutions would be seeking solutions in data privacy and information management. Moreover, “The rash of high-profile data security breaches in 2005, supported by the survey respondents’ admissions that 18%

of them have experienced some form of data leakage, has exposed deeply rooted and long-term problems in the way FIs¹⁰ have been managing their sensitive customer data” (p. 14). In New Zealand such breaches have been reported in the media. In 2008, Ticketek accidentally emailed the personal details of 918 customers (Newton, 2008). The incident was detected through Ticketek’s “fraud-monitoring system” and “an investigation found the credit card processing system had malfunctioned” (Newton, p. A4). Customer concern was centered on the fact that Ticketek’s first point of contact, their call centre, appeared unconcerned and advised that nothing could be done until after the weekend – a delay of three days. In 2009, hackers stole the personal information of 6000 Shell customers. This affected 1400 customers in New Zealand and 4500 customers in Australia (“Hackers hit Shell”, 2009). The stolen information was that which customers supplied on application for their Shell card and contained not only name and contact details, but in some cases bank account details. Shell contacted all those concerned.

These identity fraud related media reports described above are not isolated incidences in New Zealand. Table 2 provides a mere sample of media headlines relating to identity fraud in New Zealand.

Table 2: A Sample of New Zealand Related Identity Fraud Headlines

Police vow to resolve man’s identity theft nightmare (Stuff.co.nz, 1 June 2005)
Identity theft shreds nerves (Stuff.co.nz, 6 November 2005)
Spies prompt law overhaul (The New Zealand Herald, 7 March 2006)
Deported MP came back illegally (The New Zealand Herald, 14 August, 2006)
170 passport fraudsters make it to NZ (Stuff.co.nz, 21 August 2006)
Student used false papers to get loan (Stuff.co.nz, 25 August 2006)
NZ passports being used illegally (The New Zealand Herald, 27 September 2006)
Fraudulent passport lands Nelson man in prison (Stuff.co.nz, 4 October 2006)
Kiwis concerned over identity theft (Stuff.co.nz, 29 April 2007)
Wake-up call over identity theft (Stuff.co.nz, 30 April 2007)

¹⁰ The acronym ‘FIs’ stands for Financial Institutions.

Super cards could pose threat of identity theft (Stuff.co.nz, 10 May 2007)
The real cost of identity theft (The New Zealand Herald, 12 May 2007)
Bite on face leads to fraud charges (News.com.au, 16 May 2007) ¹¹
National's shameful record with immigration fraud (beehive.govt.nz, 28 June 2007)
Critics pan bill to tighten access to public documents (Stuff.co.nz, 25 July 2007)
Hospital suspects passport fraud (Stuff.co.nz, 26 July 2007)
The man who faked his own death (Stuff.co.nz, 30 July 2007)
ID theft is on the increase (Herald on Sunday, 12 August 2007)
Criminal returns on visa (Herald Sun, 13 August 2007)
Kiwis worried by online identity theft, fraud – survey (Radio New Zealand News, 21 August 2007)
How private is your life? (New Zealand Listener, 18-24 August 2007)
Man fined for passport forgeries (Stuff.co.nz, 29 August 2007)
Iraqi's details hidden (nzherald.co.nz, 8 September 2007)
Woman in court over alleged dead baby identity scam (Radio Live, 10 September 2007)
\$3.4m benefit fraudster jailed for 8 years (Stuff.co.nz, 12 October 2007)
Identity theft renews grieving for lost baby (Stuff.co.nz, 15 December 2007)
Jail sentence inevitable for identity thief: judge (Stuff.co.nz, 3 April 2008)
Losing face through fraud on the internet (Weekend Herald, 26 July 2008)
10 NZers buy fake online degrees (Weekend Herald, 16 August 2008)
Name change to conceal criminal record 'too easy' (Stuff.co.nz, 2 November 2008)
Giving false details a bad move – police (Stuff.co.nz, 3 November 2008)
The cost of losing yourself (Stuff.co.nz, 18 November 2008)
Akld millionaire under citizenship microscope (Stuff.co.nz, 22 November 2008)
Scammers steal \$35k from skimming ATM (Stuff.co.nz, 14 December 2008)
'Space fakers' spark identity theft concerns (Stuff.co.nz, 5 January 2009)
The renaming of names (Stuff.co.nz, 12 January 2009)
Women the new pimps in human trafficking trade (Stuff.co.nz, 13 February 2009)
Researcher questions government security analysis (Computerworld.co.nz, 16 February 2009)
Identity-fraud warning after passports lost (nzherald.co.nz, 26 February 2009)
Online scams costing Kiwis dearly (Stuff.co.nz, 2 March 2009)
Police ask for help nabbing fraudster (nzherald.co.nz, 3 March 2009)
Police struggle to handle fraud (Stuff.co.nz, 9 March 2009)
Hackers steal Shell customer details (nzherald.co.nz, 17 March 2009)
Size of clerk's fraud justifies sentence (Stuff.co.nz, 19 March 2009)
Big brother watching our lives online (Stuff.co.nz, 4 April 2009)
SSC reviews identity project (Stuff.co.nz, 20 April 2009)
Party used to sell fake passports (Stuff.co.nz, 17 June 2009)
Warning to beware of passport scam (Scoop.co.nz, 18 June 2009)

¹¹ A repossession agent was bitten on the face by a man whose car he was attempting to repossess in Sydney, Australia. Consequently, the New South Wales Police were called and the car was searched. In addition to several credit and debit cards, three false New South Wales driver's licences and two New Zealand driver's licences in different names were located. The man faced 26 charges for fraud and one for assault.

The importance of identity fraud existing in any system is related to the fact that it is a breeder crime, in that it enables other crimes to be committed while the offender is undetected. Beardsley (2004) states:

Once all the necessary documents have been fraudulently reproduced either in support of a stolen identity or the creation of a new one, the offender is free to go about illegally obtaining money, loans, benefits or entitlements and undertake business dealings, with little risk of being detected. (p. 45)

Therefore, for an offender, it is much easier and more anonymous to commit identity fraud in order to steal money from someone's bank account, rather than to rob a bank in person where the risk of capture is far greater and the police have security footage of the individual. Identity fraud also has the benefit of being able to be applied across industries, making resolutions for the problem somewhat haphazard in nature. Any systemic fixes for identity fraud are complex, as the following example in relation to the United States border demonstrates:

Before September 11 2001, the government's list of suspected terrorists banned from air travel totaled just 16 names. There are now over 44,000 passengers on the no-fly list, while the selectee list contains at least 75,000 names. Some of the most dangerous terrorists are never listed on either of the watch lists, as the intelligence agencies that supply the names do not want them circulated to airport employees in foreign countries for fear that they could end up in the hands of the terrorists ... The concept of a no-fly list is premised on the idea that the government knowing who someone is can make airports safer. This idea is not universally accepted, and there are many researchers and commentators who strongly disagree with it ... In fact, the very definition of a "suicide bomber" means that there cannot be repeat offenders. (Soghoian, 2008, pp. 5-6)

The above example raises the following questions:

- How does the United States government deal with false positive matches, that is, people who hold the same identity details as someone who is on the watch list, but is not that individual?

- Should the majority of air travellers be affected by the criminal actions of a few?
- If intelligence agencies do not want foreign airport employees to have access to the watch lists, how are any identity fraudsters meant to be prevented from boarding an aircraft to the United States in the first place?
- At what cost does this system come for both the passenger and the Government?
- Has the name been spelt correctly? Transcribing names from other languages into English is often not accurate and some names can be spelt in more than one way. There is also the risk of data entry errors.

In New Zealand, INZ largely overcomes these problems through the use of a system named Advanced Passenger Processing (APP). Airline employees are not provided with a copy of a 'watch list', but will receive a 'Do not board' message if there is a problem with the passenger. In addition, Identity Services, a business group of the DIA in New Zealand, administer the Watch List of people's images that it has good cause to believe may apply for a false New Zealand passport. This system is for internal use only and works with facial recognition technology. Every individual who applies for a New Zealand travel document has their image compared to those held on the Watch List. However, governments from around the world cannot relax on the technology front as the counterfeiters and forgers eventually match or come close to matching the technology and "aggressive and inventive adoption of new technologies has helped traffickers to lower risk, increase productivity, and streamline their business" (Naím, 2006, p. 21).

Potentially, the greatest harm resulting from a New Zealand Government systems failure in the identity arena is that of its international reputation and integrity. Ladley and White (2006) advise:

Identity fraud is growing in prevalence, and it poses risk to New Zealand in terms of protecting both our own borders from illegal immigrants with false documentation and the reputation of our own documentation as trustworthy. There is a risk that we disadvantage our citizens if New Zealand border agencies are seen to be insufficiently vigilant in ensuring documents are genuine. The integrity of our systems affects our international reputation, which in turn is critical to effective facilitation of the flow of people. But secure identity documents depend on other states' capacities to recognise the documents (e.g. by common electronic systems) and/or their willingness to accept them as valid. (p. 29)

However, despite New Zealand's best efforts to keep identity fraud at bay, it faces challenges from some of its closest neighbours in the South Pacific. Small island nations do not have resources such as funding, technology, knowledge or manpower to prevent many incidences of identity fraud. In fact, the state of some of these countries enables identity fraud to prevail. Tagicakibau (2005) wrote:

Illegal immigration, passport scams, organised crime, slack border controls, in addition to arms, drug and people smuggling, are causes of concern in the Pacific ... Many are worried about the short-sighted sale of passports and citizenship by their governments to unknown foreigners for easy money. (p. 195)

While the selling of passports and citizenship may seem an abhorrent concept in New Zealand, it is common in some Pacific Island countries. Ironically, there are provisions in New Zealand legislation that support such activity. For example, in order for a child to obtain New Zealand citizenship by birth, one of its parents must either hold New Zealand citizenship or permanent residence at the time of the child's birth. Alternatively, one of the parents must have the entitlement to reside permanently in Niue, Tokelau or the Cook Islands (Section 6, *Citizenship Act 1977*). When countries such as Niue are selling their permanent residency to Chinese nationals for money, it is

a 'backdoor' method for non-New Zealand permanent residents or non-New Zealand citizens to gain New Zealand citizenship for their child. In terms of identity fraud, the New Zealand Government is deferring to a foreign, less developed country with far less state regulatory power and resources, in order to conduct the appropriate security and identity checks on the parents of the child. Furthermore, if the parents of the child are, or become, overstayers in New Zealand, the fact that their child has New Zealand citizenship is taken into account in the 'humanitarian interview' conducted by INZ and may affect the decision as to whether to remove them from New Zealand. All actions have consequences in the system and some of these may be more sinister as described by Bennett (2005):

Even the less dramatic issuing of Solomons passports could open the path for the terrorists and organised crime syndicates. Selling passports has appealed to desperate Solomons governments in the past. (p. 438)

While New Zealand's decision to write Niue, Tokelau and the Cook Islands into Section 6 of the *Citizenship Act 1977* may be based upon foreign policy, humanitarian or trade policy, it surely undermines New Zealand's own security policy. The *Organised Crime Strategy 2008-2009* (New Zealand Ministry of Justice, 2009) reported:

Identity crime is an increasing component in many offences in New Zealand, often acting as a precursor or enabler to other serious crime. Fraudulent and stolen identities can facilitate organised crime for example, multi jurisdiction fraud, people trafficking and money laundering. (pp. 8-9)

The public acknowledgement by the New Zealand Government that identity fraud is a problem in this *Strategy*, has opened the gate for the development of a policy framework in this area. However, simultaneously, New Zealand has over 100 public registers, some of which provide personal details about other members of the public to anyone in New Zealand. Commonly known examples of these registers include the births, deaths and marriages register, the motor vehicle register, the companies

register, and the electoral roll. These registers enable any member of the public to obtain personal information about an individual. The report entitled *Public Registers* published by the New Zealand Law Commission (2008) stated “technology has also made it possible to readily combine publicly available information held across a range of databases, to create a profile of a particular individual” (p. 11). Such registers thus facilitate identity fraud and are a weakness in New Zealand’s systems. In the same report, the Law Commission stated:

Identity theft was cited by the Department of Internal Affairs as a concern underlying the recent proposals to amend the Births, Deaths, and Marriages Registration Act 1995, because key pieces of information required to steal a person’s identity are their full name, date and place of birth, and their parents’ names. All of this information is readily accessible on the register of births. However, during consultation, the Police indicated that they do not know how much information used for the purpose of identity crime is sourced from public registers. Access to the equivalent Australian registers has been restricted for several years, without the incidence of identity theft declining. (p. 67)

The fact that the New Zealand Police held no recorded statistics of how many identity crimes had been committed as a result of information held on public registers, does not negate the fact that public registers can be and have been abused in this manner. Similarly, the Australian experience indicates that other modus operandi have now been utilised since the closure of the registers and that identity crime may have risen in popularity in general, as other literature on this topic has suggested. Due to the closure of the Australian registers, it is impossible to calculate the cases of identity fraud that the closures have prevented from occurring.

When the *Births, Deaths, Marriages and Relationships Registration (BDMRR) Amendment Bill* was still being debated in the public arena in New Zealand, one of the key contributors in the debate was the New Zealand Society of Genealogists. Genealogists in New Zealand wanted to retain the ability to access the Births, Deaths

and Marriages Registers in order to conduct genealogical research. However, they would still be able to do this if the registers were kept open and they were given access to printouts of register information only. There was no need for the New Zealand Government to continue providing certificates to the general public upon payment.

Nonetheless, when the *BDMRR Act* came into effect on 25 January 2009, the New Zealand Government still made it possible for a member of the public to obtain another person's birth, death or marriage certificate. The only difference was that whoever ordered the certificate now needed to provide a form of identification when placing the order and a referee needed to verify the identity of the person who ordered the certificate. However, this system relies on the fact that a genuine identity document is going to be provided and that a referee is going to tell the truth. While the order form states that the referee must be from a specific group such as a Kaumatua, a Police Officer, a Minister of Religion, it is unlikely that any verification is going to occur to establish whether this is the case. There is warning on the order form to both the person ordering the certificate and the referee which states:

Warning: It is an offence, punishable by imprisonment and/or a fine of up to \$10,000, to make a false statement to obtain a certificate, printout or any other document, or to provide any means of identification knowing that it is false or is suspected to be forged or falsified. (New Zealand Department of Internal Affairs, 2009a)

As previously noted, identity fraud occurs with speed and often for considerable financial gain. Unless any false identity document is discovered immediately, the person ordering the document is likely to succeed in committing this crime and a short prison sentence or a \$10,000 fine is hardly a deterrent when infinite gains can be made from obtaining someone else's birth certificate. Moreover, if the person supplies a false driver's licence as identification and also provides a referee who does not exist, then

actually locating the person to prosecute them is unlikely. Another change to the *BDMRR Act* was that a register was going to be kept of any person who ordered a certificate under an individual's identity. This enables anyone to request to see this register. Again, this may act as a small deterrent but there could be a time lag between when someone orders one's birth certificate and when one discovers that they have done so. Any number of crimes could be committed in an individual's identity in this period, not only in New Zealand but also overseas.

The taking of another's identity, as described above, is just one avenue that identity fraudsters can use. Key informants that were interviewed expressed concern at the ease at which an individual can change their own name in New Zealand. In my own experience, these views are regularly echoed throughout the public and private sectors. The *BDMRR Act* has now meant that foreign nationals can no longer change their name in New Zealand unless they are a New Zealand citizen or permanent resident. Any birth certificate issued after 25 January 2009 will show the new name as well as "all previous names", according to the *Name Change by Statutory Declaration* BDM120 form (New Zealand Department of Internal Affairs, 2009b, p. 2) which outlines information relating to name changes by statutory declaration. However, there is only sufficient space on the birth certificate to list 10 names. Some individuals have more than 10 name changes. Section 2 of the *Name Change by Statutory Declaration* application form (BDM120) refers to one's name being 'abandoned' and a new name being used. In my experience, some individuals continue to use their previous name as well as their current name to suit their own purposes. Reasons for this can range from obtaining a passport from one's birth country in one name and a New Zealand passport in another name, or using a name change to commit fraud against financial organisations. Despite all of the identity fraud that can originate from Births, Deaths

and Marriages, they do not *freely* share information with other public sector agencies who are attempting to uphold the law.

A most concerning issue relating to identity fraud in New Zealand is the lack of understanding in relation to identity fraud shown by politicians. In the third reading of the *BDMRR Amendment Bill*, now former Member of Parliament for the National Party, Brian Connell (NZPD, 2008) stated:

So why does the Government want to do this? First, we were told by the Minister that it was to stop identity fraud. That is a smokescreen if ever I have seen one. Just a cursory investigation of the evidence about identity fraud in this country blew that argument right out of the water. Officials quote something like only six to eight cases in our recent history, and I think I am making a very liberal interpretation of evidence that they presented to the committee. I do not think that it was even as many as that. (p. 17298)

While the lack of official statistics on identity fraud in New Zealand may have not assisted the Government's case, the attitude of Brian Connell is ignorant. Reports from other similarly democratic governments published prior to Brian Connell's comments all point to a prevalence of identity fraud and aim to work toward finding solutions. *An Agreement to a National Identity Security Strategy* developed by the Council of Australian Governments (COAG) (2007) stated:

Identity security is a critical concern to Commonwealth, State and Territory governments which have responsibility for Australia's national security, revenue protection and law enforcement. False identities underpin some terrorist and criminal activity and undermine border and citizenship controls and efforts to combat terrorist financing and financial crime. Identity theft is also a major invasion of privacy and a serious concern to the Australian community. (p. 7)

The United States General Accounting Office (GAO) stated in their 2002 report entitled *Identity Theft: Available Data Indicate Growth in Prevalence and Cost*:

Although not specifically or comprehensively quantifiable, the prevalence and cost of identity theft seem to be increasing, according to the available

data we reviewed and many officials of the public and private sector entities we contacted. Given such indications, most observers agree that identity theft certainly warrants continued attention, encompassing law enforcement as well as prevention efforts. (p. 1)

The Home Office in the United Kingdom published their report in December 2006 entitled *Border, Immigration and Identity Action Plan: Using the National Identity Scheme to Strengthen Our Borders and Enforce Compliance Within the UK* and stated:

We face threats from identity fraud, illegal immigration, organised and international crime and global terrorism. We have put in place measures to respond to them, and will continue to do so as they evolve. (p. 4)

In March 2007, the Canadian Internet Policy and Public Interest Clinic (CIPPIC) from the University of Ottawa wrote in its report entitled *Identity Theft: Introduction and Background*:

Why has identity theft become such a gripping issue, compared with other types of crime? Any form of crime has negative financial and other consequences for its victims, but those associated with identity theft can be particularly hard hitting. (p. 3)

Identity theft is not just a problem in its own right. It also has ramifications for other types of crime. United States and Canadian law enforcement agencies report a growing trend in both countries toward greater use of identity theft as a means of furthering or facilitating other forms of fraud, organized crime (the bulk of identity crime is committed by organized crime) and terrorism ... Especially troubling is the now established link between identity theft and national security. (p. 4)

Given the serious nature attributed to identity fraud in other western democracies and given that in New Zealand there has been a lot of publicity in relation to online scams alone, it is unfathomable to consider that identity fraud does not exist in New Zealand. Equally it is disturbing that officials could only provide evidence of such a few cases when I alone, could name so many more. It raises questions as to the basis upon which these cases were selected for special mention, while many others were not reported. It also raises the question as to who was asked to provide this data. A check with frontline officers who work in the identity fraud arena would have revealed more than

the six to eight cases presented to Parliament. In the same reading of the *BDMRR Amendment Bill*, Member of Parliament, Metiria Turei (NZPD, 2008) from the Green Party stated:

We agree that the Government was right to be worried about identity fraud, but there was not that much evidence that the Births, Deaths, and Marriages database was much of a source of false identities. The main problem with identity fraud is that many private agencies in New Zealand are slack when checking identities, and the law cannot substitute for those agencies getting their act together ... on various databases, and any agency can ask any applicant for a credit card, or for whatever, plenty of tricky questions so that he or she would have to be the genuine person to be able to answer them properly. (p. 17298)

The above comment also reveals a lack of understanding by the Green Party. BDM do not consider it their 'job' to uncover or report fraud, but merely to register life events. Based upon this premise, who is in a position to collect such data on identity fraud from BDM? The fact that there "was not that much evidence" (NZPD, 2008) does not mean that there were no cases of identity fraud. Metiria Turei has failed to acknowledge the potential damage caused by BDM products as breeder documents for other crimes. Moreover, abuse of BDM products may occur in jurisdictions outside of New Zealand or they may occur many years later. As to the comment that private agencies "are slack when checking identities" (NZPD, 2008), the system in New Zealand does not allow private agencies to conduct checks against public sector databases as they are largely told that this is against the *Privacy Act 1993*. For a private organisation to merely ask for a credit card to confirm identity is naive, given the skimming technology that exists nowadays which allows an individual to replicate another individual's card details. Finally, with the amount of personal information that is available through the Internet or other sources such as dumpster diving, it is not difficult to answer personal questions when asked. Should the above politicians' comments in relation to identity fraud be representative of the National Party and

Green Party sentiment, developing and implementing public policy relating to identity fraud in New Zealand faces many challenges from the top down.

4.4 POLICY AND LEGISLATION

4.4.1 Policy

Anderson et al. (2008) stated: “Public awareness of identity theft as both a personal threat and a public policy issue has increased substantially” (p. 171). Moreover, the Victorian Ombudsman (2007) in Australia stated in their report entitled *Investigation into VicRoads Driver Licensing Arrangements*, that the Australian Federal Police had advised:

- Identity fraud is presenting a growing threat throughout the world and a false identity provides a means of committing a wide range of criminal activity.
- Issuing agencies world wide are interdependent on the integrity and process each maintains.
- Most government agencies and financial institutions have significantly upgraded their ‘security of identity’ where the client receives a benefit from proving their identity. (p. 29)

However, the New Zealand Government is faced with a myriad of policy issues when attempting to deal with the identity fraud evolution. In brief, some of these issues include technology; organisational data reliability and validity; privacy; interagency co-operation and information sharing; resourcing in terms of feasibility, cost and measuring efficiency and effectiveness of systems; jurisdiction; difficulties in overseas document verification; outcomes; domestic and international politics; proactive versus reactive measures; risk versus facilitation and custodial issues relating to who ‘owns’ a policy. Pontell (2002) pointed out, “It is clear from both the U.S. and Australian experience at least, that identity fraud poses serious challenges and policy choices that generally center on issues of cost and control” (p. 4). These policy issues can be as

complicated as the system of identity fraud itself. Davies and Hosein (2007) acknowledged this point in stating: “Identity policies, as with all sophisticated and complex policies, have contentious components” (p. 3) and “Like most policies that involve advanced social, legal, technological and economic issues, identity policies are complex” (p. 5).

In New Zealand, an example of political and social contention is described in Ian Wishart’s book, *The God Factor*. Written in 1999, it outlined both the political and social push and pull factors in New Zealand in relation to the introduction of the digital driver licence containing an individual’s photo – the current driver licence that is used today in New Zealand. There were fears that the New Zealand driver licence would become a de facto national identity card. Consequently, the Government restricted access to driver licence photos to New Zealand Transport Agency staff only and to the New Zealand Police in cases involving traffic issues. Despite the fact that the driver licence in New Zealand has become a de facto identity card the ‘old rules’ still apply. This means that the New Zealand Transport Agency is unable to provide photographs of criminals or suspected criminals to other public agencies who are attempting to maintain the law. It is ironic that the public system is impeding law enforcement by one of its own agencies and this undermines the mandate of the New Zealand Government to address issues in a ‘whole of government’ approach as promoted by the New Zealand State Services Commission (2001). In his book on the global illicit trade, Naím provided an example of the contradiction in government policy: “While the U.S. federal government is cracking down on illegal aliens, many states are giving them driver’s licences” (2006, p. 184). Similarly in New Zealand, overstayers can readily

obtain an IRD¹² number to enable them to work and pay taxes in New Zealand, even though they are not legally in the country. In addition, individuals can obtain IRD numbers in identities other than their own and can also obtain New Zealand driver licences.

Ironical as it may sound, some current New Zealand Government systems and policies facilitate identity fraud offending. Naím (2006) warned that the ways in which governments are structured is cause for concern in responding to the likes of organised criminal activity:

Bureaucracies tend to be organized in rigid, hierarchical fashion, making them less nimble in sharing information or coordinating efforts with others outside their vertical lines of command ... their dependence on standard operating procedures ... these standards create stability, predictability, transparency, and homogeneity in government operations. But they are also the source of much rigidity and slow down the response time to unanticipated circumstances. (p. 182)

Nonetheless, the establishment of centralised and regional inter-agency law enforcement groups in New Zealand such as OFCANZ¹³ and CLAG¹⁴, attempt to mitigate this risk by sharing resources and intelligence, communicating regularly, conducting joint operations and finding common solutions to problems. What the New Zealand Government has been lacking has been the nomination of a public sector agency to take control of the problem of identity fraud. While the New Zealand Police administer a database of misused or fraudulent identities, it is the DIA (Identity Services) that has undertaken the main work on identity in New Zealand (for example the EOI Standard, the Identity Assurance Strategy, the Data Validation Service and the Identity Verification Service). DIA's role in the identity arena is continually evolving but should they become the custodian of identity policy in New Zealand, they need to

¹² IRD is an acronym for Inland Revenue Department.

¹³ OFCANZ is an acronym for Organised and Financial Crime Agency of New Zealand.

¹⁴ CLAG is an acronym for Combined Law Agency Group.

ensure that any policy addressing identity fraud can be successfully applied to all public sector agencies and ultimately, the private sector. Whitley and Hosein (2008) stated:

The choice of government department that designs the policy on this issue directly influences the kinds of approaches and other policy agendas enrolled in the solution. The response and emphasis of a department of consumer affairs is likely to be very different from that of a department with policing responsibilities and will differ from departments responsible for trade and industry. (pp. 98-99)

An additional challenge facing the development of public policy in the identity fraud arena in New Zealand is the absence of reliable and valid statistics. Without such empirical data, comprehensive development of public policy is difficult. The United Nations Intergovernmental Expert Group (OECD, 2009) conducted a study into identity fraud. In a meeting on 2 April 2007, they stated:

The available evidence clearly suggests that economic fraud is a serious problem, and is increasing, both globally and in a number of Member States. However, many States reported that they do not have accurate information or a systemic framework for gathering and analysing such information ... Data that would permit the quantification of fraud by occurrence or offence rates are not available in many States, almost no official data quantifying proceeds exists ... There is growing awareness of and concern about identity-related crime, but it represents a novel concept for law enforcement and criminal justice experts in many States. There are few legislative definitions and many basic concepts remain fluid at this early stage. (p. 100)

And

Close collaboration between relevant public and private sector entities in developing and implementing preventative measures will also be important for success ... It is therefore recommended that Member States develop and implement effective fraud-prevention measures, at the national, regional and global levels, and in co-operation with the private sector. (p. 102)

Traditionally, the *Privacy Act 1993* has prevented the public sector from sharing personal information with the private sector and this is a big hurdle to overcome if

preventative identity fraud measures and policies are going to be developed in New Zealand. The *Organised Crime Strategy 2008-2009* (New Zealand Ministry of Justice, 2009) supported this point in saying “information sharing has sometimes been unduly restricted due to the differing and conservative interpretation of privacy laws” (p. 10). Fuelling the policy issue is that there is no framework to support the mandatory provision of identity fraud statistics by public sector agencies or private sector organisations. While it has been reported that “all types of identity related fraud are growing rapidly” (Crosby, 2008, p. 27), with the exception of DIA (Identity Services), there are no specific outcomes or discussion on identity fraud in the annual reports or statements of intent of the following agencies whose products and services can be affected by identity fraud:

DIA: In the New Zealand Department of Internal Affairs (2008) *Annual Report 2007-08*, the Chief Executive states that the key outcome relating to identity, “New Zealand’s approach to identity is trusted and well led ... was changed from ‘trusted records of New Zealand identity’ in 2007/08 to better reflect the Department’s leadership role in this area” (p. 2). As part of this leadership in identity, DIA (2006) focused on their custodianship of the EOI Standard “which is expected to lead to greater consistency in identity verification processes for New Zealanders dealing with government agencies” (p. 27) and “we plan to progress the EOI Standard to the next level of the e-Government Interoperability framework (e-GIF) to become a ‘Recommended’ standard” (p. 2). The Chief Executives reported that “the IVS¹⁵ will provide the public with a way to verify their identity online, and in real time, when seeking services from a government agency” (p. 2). It is anticipated that the IVS will be completed in 2010-

¹⁵ IVS is an acronym for Identity Verification Service.

2011. However, in managing identity, the DIA states that it is required to 'balance' the following three factors:

- (1) The protection of the privacy and safety of citizens and other individuals;
- (2) Facilitating fair and equitable access to rights, services and entitlements;
- (3) The delivery of effective and efficient governance. (p. 27)

In summary, the DIA is working on the following areas of identity that will assist in reducing identity fraud: the EOI Standard, the Identity Assurance Framework; the Cross-Governance Biometrics Group; IVS; Border Sector Initiative; the Passport Redevelopment Programme; DVS¹⁶ (pp. 27-30). As its name suggests, the Identity Services business group of the DIA's core business is identity. In order to give some perspective, the following statistics reflect the numbers of identity documents or services requiring identity verification for 2007-2008:

- 412,636 passports and other travel documents were issued
- 118,923 births, deaths, marriages and civil unions were registered
- 262,122 birth, death, marriage and civil union certificates and printouts were issued
- 27,624 applications for grant of citizenship to foreign nationals were recommended to the Minister. (p. 28)

In terms of "Priorities for the Future", the DIA has listed seven areas in which it is concentrating on identity. These include ongoing work on the Passport Redevelopment Programme which will upgrade security from the current New Zealand passport and the implementation of new technology to run the passport system; implementation of the IVS to enable the public to verify their identity to the New Zealand Government; implementation of the DVS which will allow other government agencies to verify DIA identity documents; the review, promotion and implementation of the EOI standard across government agencies; the provision of leadership across the New Zealand Government and internationally on identity matters as well as the implementation of

¹⁶ DVS is an acronym for Data Validation Service.

the Identity Assurance Framework; auditing birth and death records; implementation of changes relating to the new *Births, Deaths, Marriages and Relationships Registration Amendment Act*. However, despite the large amount of strategic work aiming to reduce identity fraud, the performance indicators detailed in the *Annual Report 2007-08* under Vote Internal Affairs 'Identity Services' do not exactly correlate to this work. The performance indicators are divided between the three business units in Identity Services: Citizenship, Passports and Births, Deaths and Marriages. They pertain to quantitative indicators relating to timeliness standards, the numbers issued and the error rate (pp. 68-69). The error rate per se cannot be accurate when identity fraud is often detected years later, for instance, in the case of a false passport. There are no performance indicators around identity fraud. Identity is a category within the 'Policy Advice – Internal Affairs' section of Vote Internal Affairs. It is not specifically referred to in the performance indicators (p. 73). Moreover, the New Zealand Department of Internal Affairs (2007) *Statement of Intent 2007-10* states that the intermediate outcome of "Identity services are reliable and accessible and meet New Zealand and international standards" is measured by Customer Satisfaction surveys and that the "Output/Deliver Measures We Use" are "Timeliness measures" and "Customer Satisfaction" (p. 51). It is debatable as to how timeliness standards and the opinions of the general public provide a robust reflection of the identity fraud problem in New Zealand. In addition, it is unlikely that an identity fraudster is going to complain about the inaccuracy of the data on the false passport that he/she has just been issued.

DOL: Identity fraud was indirectly addressed in the intermediate outcome called "Our Place in the World" in the New Zealand Department of Labour (2008) *Annual Report* (p. 13). One of the key focus areas of which identity fraud would form a part is "Border

Security Arrangements that Manage Risk” (p. 13). This area includes achievements during the year in respect of identity related activity such as risk profiling, keeping high-risk people out of New Zealand, moving risk off-shore through APP, holding joint workshops with Australia on lost and stolen passports and the DOL leading the “Identity at the Border for Facilitation, Protection and Partnership work programme” (p. 18). In addition, Stage 2 of a business case to Cabinet received approval and funding for the following components of the Immigration Business Transformation (IBT) programme which would assist in the prevention and detection of identity fraud: Biometric identity management, upgrading risk profiling methodology, placement of 12 staff at airports with direct flights to New Zealand, increased onshore fraud resources, additional verification officers (p. 17). Moreover, New Zealand Department of Labour (2009) *Statement of Intent 2009/10-2012/13* acknowledged that the current “immigration system needs to be strengthened. The new Immigration Act will provide the basis for a more efficient system” (p. 2). Measures needed to improve the current system include “implementing the findings of the Office of the Auditor General and the State Services Commission” (p. 2) in relation to immigration identity fraud. Notably, identity fraud does not form part of the discussion on Strategic Direction while “using targeted immigration to meet critical skill shortages in some industries” (p. 8) does. In fact, identity fraud is not directly mentioned in any of the Progress Indicators relating to outcomes. The closest indicators that may include an element of identity fraud are “The number of people who enter New Zealand that do not meet criteria” and “The number of migrants deported as a result of criminal conviction” (p. 13).

LTNZ: The Land Transport New Zealand (2007) *Annual Report for the year ended 30 June 2007*, stated that in the 2006-2007 financial year, 564,000 driver licences were issued in New Zealand and that one of the key regulation and service delivery areas

was driver licensing (p. 15). Despite the issuance of such a large number of driver licences, and that this was a key result area, the Policy and Planning Group did not cite any activity in relation to driver licensing in their “Highlights and achievements 2006/07” (p. 21). In addition, in their list of 14 “Intentions for 2007/08”, the only mention of driver licensing was “Commence rules on traction engines, and amendments to Rules on road users, traffic control devices, dangerous goods, fuel consumption information and driver licensing” (p. 22). The term “rules” is vague at best and there is no indication that the security or processing of driver licences was going to change for the better in a bid to prevent identity fraud. However, while the Regulatory Services Group also did not mention driver licensing in any of their “Highlights and achievements” (p. 27), identity fraud risk was addressed twice in their list of “Intentions 2007/08”. They stated: “Commence work across the motor vehicle register to reduce the creation of multiple identities” and “Assess the profile and risk of driver licence enrolment processes against the whole-of-government Evidence of Identity standards” (p. 28). The two output classes that include driver licensing and potential identity fraud are “Regulatory implementation and enforcement” (p. 37) and “Licensing activities” (p. 39). The former output class states that LTNZ will “develop standards and procedures, monitor and audit” driver licences (p. 37) and the latter will “maintain the currency and integrity of licence-related data in statutory registers” (p. 39). Nonetheless, the term identity fraud is not cited at all in the annual report. In Land Transport New Zealand (2006) *Statement of Intent 2006-2009*, despite the prevalence of identity fraud, it is not mentioned in the section entitled “The operating environment” (p. 7). Under the “Licensing drivers” section of the “Key regulation and service delivery areas”, their activities are as follows: “Rules for removal and re-entry of drivers from/to the system for medical reasons and for court based offences”,

“Theory and practical testing of novice car drivers, drivers from overseas and heavy vehicle drivers” and “Maintaining the driver licence register” (p. 13). Once again, there is no mention of identity fraud. From a list of 22 “Key strategic initiatives”, only one potentially related to identity fraud: “Investigate creating a single customer identity for customer transactions” (p. 15).

MSD: Identity issues have been addressed in the Organisational Health and Capability section of the New Zealand Ministry of Social Development (2008) *Annual Report 2007/2008*. Ministry of Social Development (MSD) states that they “are providing active representation on Steering and Working Groups” for the Identity Verification Service and that this Service “proposes to provide government agencies with a high level of confidence regarding the identity of the online user, while placing people in control of the transaction and protecting their privacy” (p. 29). In addition, on a broader level, fraud is referred to in the Managing Performance and Integrity section of the *Annual Report*. Of potential relevance to identity fraud, MSD stated that they “investigated more than 15,000 cases of potential benefit fraud” and they “compared more than 12 million records through data matching with other agencies to detect incorrect benefit payments” (p. 32). However, in New Zealand Ministry of Social Development (2009) *Statement of Intent 2009-2012*, from the nine priority areas, there is no mention of identity fraud being a priority. Furthermore, identity fraud is once again not mentioned in any of the six outcome areas. This is ironic given that New Zealand’s biggest benefit fraudster, Wayne Thomas Patterson, used more than 100 identities to obtain \$3.4 million in benefits and was convicted on 31 March 2008 (*Wayne Thomas Patterson v The Queen*) in the 2007-2008 financial period of the *Annual Report*. There is no reference to the Patterson case in either the *Annual Report* or the *Statement of Intent*.

NZCS: From July 2008, the Border Sector Chief Executives agreed to four priority work streams – one of which is “identity at the border for facilitation, protection and partnership” (New Zealand Customs Service, 2008, p. 13). NZCS has three outcomes: Protection, Facilitation, Revenue. Of relevance to identity fraud are the Protection and Facilitation outcomes. The Protection outcome states: “New Zealand is protected, at the border, from the entry, or exit, of people, craft, goods, Maori taonga and other treasured items, where the entry or exit may pose a material risk to our national interests” and “We protect New Zealand from harm by detecting and deterring illegal border activity” (New Zealand Customs Service, 2009, p. 15).

NZP: In the New Zealand Police (2008a) *Annual Report 2007/08*, the three outcomes that the Police focused on were: Confident, Safe and Secure Communities (p. 6); Less Crime and Road Trauma, Fewer Victims (p. 9); World-Class Police Service (p. 14). The key policy work for 2007-2008 under Confident, Safe and Secure Communities did not mention any form of identity related work. In fact, the only work reported that the Police engaged in to reduce identity fraud was under the outcome of World-Class Police Service under the Improving Technology Capability section where they stated “an interface to allow automatic processing of fingerprint requests from the Department of Corrections to assess the true identity of prisoners or visitors to corrections’ facilities was developed” (p. 15). However, the Police Electronic Crime Strategy to 2010, revealed under the outcome of Less Crime and Road Trauma, Fewer Victims, will inherently deal with electronic identity. In addition, under the outcome of World Class Police Service, the New Zealand Police have memoranda of understanding with 40 other agencies and “police actively seek out opportunities and initiatives to work with other agencies and add value by ensuring better outcomes are achieved jointly than would be achieved by each agency working alone” (p. 17). In the 16 pages

of statistical information contained in Part 7 of the Annual Report, there was only one reference to a specific identity statistic: Fingerprints Confirming Other Identity. The figures for this statistic were 960 cases in 2006/07 but only 162 cases in 2007/08. This is a drop of 83.1% over a 12 month period (p. 106). Identity crime was also not discussed in the Demand Drivers section of the New Zealand Police (2008b) *Statement of Intent 2008/09-2010/11* (p. 8). The closest association with identity fraud was under the Changes of Offending section which formed part of the Strategic Direction where it stated “The emergence and proliferation of new technologies such as computers, mobile phones and the internet, have given rise to new ways of committing offences” (p. 9). However, identity fraud was not in the list of 16 priorities of Operating Intentions (p. 14). Finally, from the three outcome groups previously stated, there were no output measures for identity fraud (pp. 15-18).

One of the recommendations of the United Nations Intergovernmental Expert Group (as cited in OECD, 2009) may assist New Zealand in establishing the ‘basics’ in order to assist in the development of a sound identity policy framework:

Systematic and structured processes for gathering and analysing data in each Member State are developed, and UNODC¹⁷ should be asked to assist in this process ... Generally, such processes should include:

- (i) A standard typology or classification framework of offences or activities;
- (ii) The gathering of qualitative and quantitative information from multiple sources, including official offence reports or complaints and other sources.
- (iii) To the extent feasible, the gathering and analysis of information about the costs of fraud. This would include ... the indirect economic costs, and the non-economic costs of fraud. (pp. 100-101)

The three processes stated above are currently what is missing in the New Zealand identity fraud puzzle: a lack of statistics, little knowledge as to how much it is costing

¹⁷ UNODC is an acronym for United Nations Office on Drugs and Crime.

the country and an absence of specific identity fraud offences. In examining what an 'identity policy' actually is, Boa, Clement, and Hosein (2006) defined it as follows:

A comprehensive national identity scheme involves the collection and processing of individual-specific data that will be shared across services, both within and beyond government, often for a wide variety of purposes.
(slide 3)

The new Identity Verification Service in New Zealand will ultimately provide identity assurance across the public sector but if identity fraud is to be minimised, the service must extend into the private sector. The *Organised Crime Strategy 2008-2009* (New Zealand Ministry of Justice, 2009) states:

Working with the private sector will support increased business awareness of suspicious activity that is linked to organised crime Working together with the private sector will provide a valuable complement to the intelligence available to law enforcement agencies, ensuring greater efficiency and effectiveness in their operations. (p. 8)

Nonetheless, the practicalities of developing and implementing an identity policy are intricate. Hosein (2008) states that there are several dynamics at play when considering identity policy:

1. There are always political risks ...
2. There are uncertain drivers for change ...
3. There is a divide between what proponents dream and what is deliverable ...
4. Choices are easily made but rarely are they effective ...
5. After the excitement of deciding upon new policies, costs always creep in ...
6. The shape of the policy is often dictated by the policy-owner ...
7. Identity policies usually cater for civil liberties and privacy at too late a stage. (pp. 3-4)

In respect of identity politics, as has been learned from the British Government's attempts to introduce a national identity card, public opposition is inherently present (Home Office, 2006). It is important that the New Zealand Government 'get it right' as Boa et al. (2006) reported:

- A successful policy can be seen as a positive renewal of the social contract.
- An unsuccessful policy can be seen as a profound lack of respect by the government toward its citizens (slide 14).

Moreover, while national policies in identity will provide a strategic and legislative focus, micro-policies to protect the consumer are imperative in the private sector. Stories of the aftermath of individuals who have had their identities stolen are common. Their issues range from having to clear soiled credit histories to proving to the justice department that they were not driving a car stopped by the Police. Clearing one's name can often take years:

There are (at least) four main policy issues associated with identity theft. First, who will pay when an identity thief steals goods? Will it be the person whose identity is stolen, the merchant targeted by the thief, or a financial intermediary – such as a credit card issuer? Second, what rules should govern the protection of consumer data? Third, what rights should individuals have to challenge or limit access to information about their identity and credit history? Fourth, as identity theft is a crime, both the legal penalties and level of enforcement to detect and prosecute it must be determined. (Anderson et al., 2008, pp. 184-185)

The next section examines the legislative issues for identity fraud in New Zealand.

4.4.2 Legislation

New Zealand has no specific legislative provisions for identity fraud. Offences involving fraud against the main identity documents in New Zealand are covered by varying pieces of legislation as outlined in the following table:

Table 3: New Zealand Legislative Acts Enforcing Identity Related Crime

New Zealand Legislative Act	Sections Covering Law Enforcement	Identity Documents Covered by Act
<i>Passports Act 1992</i>	Section 29A - Forged and false New Zealand travel documents	New Zealand passports
	Section 30 – Offences	Emergency travel documents

	<p>relating to passport information and material</p> <p>Section 30A – Improper issue of New Zealand travel document</p> <p>Section 31 – Other offences</p> <p>Section 31A – Jurisdiction in respect of actions taken outside New Zealand</p> <p>Section 32 – False representations</p>	<p>Refugee travel documents</p> <p>Certificates of identity (issued by DIA)</p>
<i>Citizenship Act 1977</i>	Section 27 – Offences and penalties	New Zealand citizenship certificates
<i>Births, Deaths, Marriages, and Relationships Registration Act 1995</i>	<p>Section 71 – Certificates to be prima facie evidence</p> <p>Section 89 – Offences and penalties</p>	<p>Birth certificates</p> <p>Marriage certificates</p> <p>Civil Union certificates</p> <p>Death certificates</p> <p>Name change certificates</p>
<i>Immigration Act 1987</i>	<p>Section 66 – Power to require surrender of documents from third party</p> <p>Section 142 – Offences</p>	<p>New Zealand certificates of identity (issued by INZ)</p> <p>Visas and permits</p> <p>Passports</p> <p>Citizenship certificates</p>
<i>Crimes Act 1961</i>	<p>Section 98C – Smuggling migrants</p> <p>Section 98D – Trafficking in people by means of coercion or deception</p> <p>Section 228 – Dishonestly taking or using a document</p>	All documents (including computer systems)

	Section 249 – Accessing computer system for dishonest purpose	
	Section 250 – Damaging or interfering with computer system	
	Section 251 – Making, selling, or distributing or possessing software for committing crime	
	Section 256 – Forgery	
	Section 257 – Using forged documents	
	Section 258 – Altering, concealing, destroying or reproducing documents with intent to deceive	
	Section 259 – Using altered or reproduced document with intent to deceive	
	Section 261 – Counterfeiting public seals	
	Section 264 – Paper or implements for forgery	

In recent years there has been a move by some Western countries to implement specific identity fraud related offences into their legislation. Examples of these are as follows:

Australia: The state of Queensland has enacted the *Queensland Criminal Code and Civil Liability Amendment Act 2007* in March 2007 and the state of South Australia has enacted the *South Australia Criminal Law Consolidation (“Identity Theft”) Amendment Act 2003* which came into force on 5 September 2004 (OECD, 2009, p. 48). In other

states identity crimes are not a “stand-alone offence” but identity security is of increasing importance in Australia (OECD, 2009, p. 48).

Canada: On 21 November 2007, a new bill making identity theft was introduced. The current *Criminal Code* covered impersonation and forgery offences but not other identity offences which involved the ‘manufacture’ and possession of identity information (OECD, 2009, p. 48).

United Kingdom: On 15 January 2007, the *UK Fraud Act 2006* was enacted. Offences against this Act include online offences and identity fraud is covered by “the act of possessing ‘articles for use in frauds’ (the term ‘article’ including ‘any program or data held in electronic form’)” (OECD, 2009, p. 48).

United States: Identity theft is a specific criminal offence under State as well as Federal law. The *Identity Theft Penalty Enhancement Act* was introduced in 2004 (OECD, 2009, p. 47). In addition, the ready availability of stolen personal information online for purchase, as well as of the equipment necessary to steal or read this information, led the United States to introduce the *Identity Theft Assumption and Deterrence Act* on 30 October 1998 (Anderson, 2008, p. 172).

Despite the above countries adopting specific identity fraud legislation, New Zealand is not in the minority in this regard. The OECD states:

Only a few OECD member countries have adopted legislation that specifically addresses ID theft. In most other countries, it is a constituent element of common wrongs, and as such it is covered by a multitude of rules including unlawful access to data, fraud, forgery, and intellectual property rights, etc. ID theft is also a facilitating factor to commit other, more serious offences. In such a case, it is often “absorbed” by the more serious offence (OECD, 2009, p. 48).

The lack of New Zealand's specific identity fraud legislation has not prevented the term *identity fraud* from being used in the New Zealand court system, as the following legal cases demonstrate:

Lee v Dept of Labour HC AK CRI 2007-404-0126 [9 July 2007]

Chee Wai Lee entered New Zealand in November 2002 and was granted a visitor's permit to remain in New Zealand until 28 February 2003. He did not renew his permit and became an overstayer. In February 2005, Chee Wai Lee was served a removal order and was removed from New Zealand on 19 February 2005. Subsequent to his return to Malaysia, he changed his name to Sin Zhe Lee, obtained a passport in this new name and returned to New Zealand on 26 August 2005 under his new identity. He made application for a student permit to stay in New Zealand under the name of Sin Zhe Lee and on the application form; he failed to advise INZ that he had previously been known as Chee Wai Lee. He also provided misleading information by stating that he had never been removed from any country. A further student permit application was made by Sin Che Lee and again he did not declare his previous identity.

Judge Stevens commented:

Counsel for the respondent submitted that **identity fraud** should be regarded as more serious than qualification fraud in the immigration and passport context. Certainly, that is the view of Immigration New Zealand (INZ), on the basis that **identity fraud** is difficult to detect, tends to involve considerable premeditation and requires the loss of a real identity and replacement by another, often accompanied by false official documents. (para. 2)

Another feature of this appeal is that it is, according to the research of both counsel, the first time the High Court has had before it an offender who has been removed from New Zealand by INZ, has returned under a different identity and provided false or misleading information to the authorities. (para. 4)

The comment by Judge Stevens (above) that this was the first case before the High Court of an offender, who has been removed from New Zealand and returned under another identity, is not representative of the fact that this sort of activity has not occurred previously. In my experience, there have been a number of similar cases in New Zealand. Judge Stevens commended the District Court Judge's (Judge Mathers) comment that "this type of offending challenged the integrity of the New Zealand immigration system" (para. 11). When considering the appropriate sentence for Chee Wai Lee, the following reference was made to Judge Priestly's comment in *Markevich v R* (2004) 21 CRNZ 41:

In the current world security climate Courts have a clear obligation to impose deterrent sentences for the use of false passports to cross frontiers with fictitious identities. So too is deterrence legitimate to underpin New Zealand's immigration controls and discourage illegal entry by fraud and deception. (as cited in para. 18)

In his discussion, Judge Stevens stipulated that identity fraud impacted upon New Zealand's immigration system and the integrity of New Zealand's borders and that this fraud was to be taken seriously by the Courts:

This country rightly places a high value on maintaining the integrity of its borders and the New Zealand immigration system. There is no doubt that immigration fraud strikes at the heart of such a system. Officials administering the immigration laws depend upon accurate and truthful information being supplied by applicants and their advisers. Whatever form the fraudulent activity may take, be it in relation to passports or qualifications, or the concealment of true identities, it is to be viewed seriously by the Courts. Parliament has mandated such an approach by the increases in penalties enacted in 2002 for breaches of the Passports Act 1992, as well as the Immigration Act. Offenders can expect deterrence and denunciation to be material factors in sentencing in all cases involving immigration fraud. (para. 31)

Dept of Labour v Ioasa HC AK CRI-2008-404-000145 [11 August 2008]

The Department of Labour appealed to the High Court against a sentence given to Tapu Ioasa which they believed to be too lenient. Tapu Ioasa, a Samoan national,

arrived in New Zealand in 1997. He was granted a three month visitor's permit on arrival and this was later extended to February 1998. Tapu loasa applied for further extensions to his permit but these were declined. He subsequently overstayed in New Zealand for a period of five years but voluntarily departed New Zealand for Samoa in April 2003. Two months later, Tapu loasa returned to New Zealand after having been granted a visitor's visa in the name of Tapu Sione. On arrival in New Zealand, he was granted a one month visitor's permit. 'Tapu Sione' departed New Zealand and returned six months later with another fraudulently obtained visa in the name of 'Tapu Sione'. In August 2004, he was approved a 12 month work permit and in that 12 month period he applied for permanent residence in New Zealand. On 21 December 2005, he was granted permanent residence in the name of Tapu Sione. In September 2006, his offending was uncovered by INZ and he confessed to the facts. Judge Singh sentenced Tapu loasa to nine months home detention and 380 hours of community work relating to five charges under the Immigration Act 1987.

Judge Priestly, in relation to the comments of Judge Singh, stated "He correctly categorised the charges as being serious, and classified the offending as "identity fraud". This comment is interesting as New Zealand law has no provision for "identity fraud" as an offence per se. Judge Priestly also noted Parliament's stance on the seriousness of offending against New Zealand's borders:

As is clear from a number of High Court decisions, in 2002 Parliament amended the Immigration Act, lifting the maximum penalty for these offences from three months imprisonment to one of seven years and the permissible fine from a maximum of \$5,000 to one of \$100,000. These significant increases are a clear unambiguous expression of Parliamentary intention about the need to preserve the integrity of New Zealand's borders and the country's linked immigration controls. (para. 26)

And

A number of High Court decisions have commented on and reflected that Parliamentary policy: see *R v Chechelnitzski* [2004] ... *Markevich v R* (2004) ... *Asamoah v Department of Labour* [2005] ... *Department of Labour v Liao* [2005] ... and *Lee V Department of Labour* [2007]. (para. 27)

Comments from the Judges in these cases reveal that the New Zealand Government is taking cases of fraud against our national borders seriously. However, the unfortunate reality is that despite the presence of such judgments, there are many cases of identity fraud that remain unprosecuted. Reasons for this include a lack of resources, a lack of interest by the Police to prosecute on behalf of other agencies who have uncovered the fraud or a fear at the border that the person on the fraudulent passport may claim refugee status. In such a situation, it is often considered more prudent to put the individual on the next departing flight rather than risk keeping them in New Zealand at the taxpayers' expense for years to come. Moreover, legislation exists in New Zealand that essentially assists identity fraudsters. Ironically, the secrecy provisions contained in Part 4 of the *Tax Administration Act 1994*, prevent IRD from sharing information that they hold with other agencies. This means that IRD officers may be aware that an individual holds more than one identity but are unable to advise other relevant public sector agencies under Section 81(1)(a) of the *Tax Administration Act 1994*. In my own experience, IRD will not share information even if an individual has given another agency their consent to make the necessary checks. The consequence of such a provision is that IRD are enabling the offender to potentially commit other crimes. Co-operation between agencies is essential if the risk of identity fraud is to be mitigated.

New Zealand's biggest case of benefit fraud resulted from MSD failing to conduct the appropriate checks with DIA. Wayne Thomas Patterson defrauded MSD of \$3.4 million of benefits, over a three year period between July 2003 to October 2006, through the use of 123 identities (*Ministry of Social Development v Wayne Thomas Patterson*, para.

24). Patterson was charged with eight counts of using a forged or false document, one count of using a document with intent to defraud and one count of using a document with intent to obtain a pecuniary advantage. In commenting on Patterson's modus operandi, Judge Woodhouse stated:

In some instances you varied the form of identification using forged temporary driver's licences, Inland Revenue numbers in the false names, bank statements from accounts opened in the false names, and false tenancy agreements you had drawn up. (para. 18)

Judge Woodhouse stated that when the Police executed a search warrant at Patterson's home address:

The following items, amongst a lot of other documents, were located hidden in the recess above the shower in your home:

- (a) 137 automatic teller machine access cards;
- (b) 102 forged birth certificates;
- (c) 56 community service cards;
- (d) 79 superannuation cards;
- (e) 125 Inland Revenue cards.

These cards and certificates were in the names of the false identities used for the frauds. (para. 10)

On 12 October 2007, Patterson was sentenced to a term of eight years' imprisonment with a minimum imprisonment period of five years. The case highlighted the lack of information sharing between two New Zealand Government agencies. A standard birth record check with DIA would have revealed issues in the identity documents that Patterson had supplied to MSD. The case also highlighted the failings of the banks in allowing Patterson to open several accounts under false identities. In terms of systemic damage, Judge Woodhouse stated: "what you have done erodes confidence in the Ministry and, more broadly, in a social welfare system designed to assist New Zealanders" (para. 24d).

The ability for an individual to change their name is enabled by the *Births, Deaths, Marriages and Relationships Registration Act 1995*. It is important in a democratic society that people have the opportunity to legally change their name. However, without some limits on this service, identity fraudsters make good use of the system to their advantage. In my experience, if one considers the reasons for an individual to change their name, it is likely to fall under one of the following four categories: (1) an individual has an embarrassing name or one that they do not like; (2) an individual is in witness protection or in fear of their life; (3) an individual has changed their gender and therefore their name; (4) an individual intends to commit fraud by changing their name – often on more than one occasion. Unfortunately, in my experience, the majority of name changes by a single individual have occurred to facilitate financial fraud.

In the private sector, legislation enhancing identity requirements for financial transactions has formed part of the recommendations by the Financial Action Task Force (FATF)¹⁸ (2009) in relation to anti-money laundering (AML) and combating the financing of terrorism (CFT). In the International Monetary Fund (IMF) country report on New Zealand in August 2005, it was stated that requirements around customer identification were contained in the Financial Transactions Reporting Act (FTRA) 1996. However, “there are no explicit requirements to identify the owners or controllers of legal persons such as companies” (p. 7). To date, this is still the case. The Companies Office, Ministry of Economic Development, requests no identification when an

¹⁸ FATF “is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering and terrorist financing. Recommendations issued by the FATF define criminal justice and regulatory measures that should be implemented to counter this problem. These Recommendations also include international co-operation and preventive measures to be taken by financial institutions and others such as casinos, real estate dealers, lawyers and accountants. The FATF Recommendations are recognised as the global anti-money laundering (AML) and counter-terrorist financing (CTF) standard” (Financial Action Task Force, 2009, p. 2).

individual establishes a company in New Zealand. They do not even request a date of birth. The obvious consequence of this is that it is difficult to take compliance action against an offender if one does not know who they are and it also allows individuals who may not be eligible to establish a company in New Zealand, to do so. The weaknesses in the New Zealand legislation relating to the financial system were summarised as follows:

The net effect is that while the FRTA provisions go some way towards implementing the necessary measures, there are a number of areas of weaknesses that need to be addressed. Identification requirements for occasional customers should cover all transactions, not just cash transactions, and equally, the various limitations and exceptions ... should be reconsidered. Guidance should be provided to financial institutions on the types of documentation that could be regarded as acceptable to verify identity. A significant weakness that needs to be addressed is the lack of adequate requirements to identify beneficial owners. The owners and controllers of legal persons such as companies should be required to be identified and verified, as should trustees and beneficiaries of trusts. Equally, if a permanent or occasional customer is suspected to be acting on behalf of another person, then there should be an obligation to identify that other person. This requirement should not be restricted to large cash transactions. (p. 7)

In order to address these FATF comments, the New Zealand Government developed the *Anti-Money Laundering and Countering Financing of Terrorism Bill 2008*. Identity related legislation is found in several parts of the Bill. Subpart 1 is entitled “Customs due diligence” and contains such sections as Section 8 – Standard Customer Due Diligence; Section 10 – Enhanced Customer Due Diligence; Section 23 – Prohibition on False Customer Names and Customer Anonymity. Subpart 3 is entitled “Record keeping” and a pertinent identity related section is Section 34 – Obligation to Keep Identification and Verification Records.

While the impending AML and CFT legislation is going to be of benefit to law enforcement in New Zealand, it will come at a cost for private sector organisations. As

stated in the IMF report comment above, it is important that guidance be given by the New Zealand Government in order for the private sector to adhere to the new legislation. Such guidance could include publishing a guide to identity documents and providing a service to the private sector through which they could verify identity, without being in breach of the *Privacy Act 1993*.

Furthermore, in terms of legislation per se, the United Nations Intergovernmental Expert Group (OECD, 2009) advocates for the development and implementation of specific identity related legislation:

While the vast majority of criminalisation issues appear to have been addressed, the evidence suggests that some specific enhancements could be considered to improve and modernise legislation ... Lawmakers need to develop appropriate concepts, definitions and approaches to the criminalisation of a range of conduct, including identity theft, identity fraud, and other identity-related crimes ... It is therefore recommended that States consider the adoption of new identity-based criminal offences. It is also recommended that, in developing new offences, common approaches to criminalisation be taken, to the greatest extent possible. (p. 101)

In New Zealand to date, the only identity specific legislation that is in development is that relating to the Identity Verification Service. However, in the *Land Transport Amendment Bill (No 4)* explanatory note it is stated that currently protection of personal information is not afforded to those people who own vehicles in New Zealand. This is due to the fact that the Registrar of Motor Vehicles has an obligation to release details, should an individual pay the required fee and provide a registration number for the vehicle. The personal details that are released are the name and address of the current owner of a vehicle and the previous listed owners of vehicles. This document reported: "Some vehicle owners are annoyed that the law, on the one hand, compels them to provide personal information to the Registrar and, on the other, obliges the Registrar to release their details to anyone who asks" (p. 3).

In respect of the above situation, the *Land Transport Amendment Bill (No 4)* proposes that the new system will still enable an individual to check whether another person is the owner of a vehicle but will merely provide a negative or positive response. No personal details will be released (p. 5).

Similarly, the *Immigration Bill 132-2 (2007)* provided for amendments relating to identity. Commentary on the Bill stated:

It is also important that citizens establish their identity and prove their citizenship at the border to access this right. (p. 1)

And

Clause 29 provides for the use of biometric information to establish a record of a person's identity, to verify identity, and to assist decision making. Many of the submissions on this clause raised general privacy and human rights issues regarding the collection and use of biometric information. (p. 2)

To improve the robustness of the border system, the *Immigration Bill* sought to collect the biometric information of departing as well as arriving passengers. Typically in the past, arriving passengers into New Zealand have received more attention than those departing. Comparative data will assist in reducing identity fraud:

The ability to collect biometric information from non-citizens departing New Zealand would reduce the risk of identity fraud. It would also make it possible to match arrivals and departures more accurately, for example when a non-citizen who was unlawfully in New Zealand departed using a false passport or identity. We therefore recommend the insertion of new clause 110A to provide for the collection of biometric information from non-citizens leaving New Zealand. (p. 3)

The development of biometrics related legislation will bring New Zealand in line with other countries around the world. While it is a start in stemming the flow of identity fraud, New Zealand still lacks an overarching identity legislation that can be applied, enacted and enforced across the private and public sectors.

5 FINDINGS

5.1 THE IDENTITY FRAUD ENVIRONMENT IN NEW ZEALAND

In New Zealand there has been little research into identity fraud. Consequently, in the first section of the interview, the 15 key informants were posed open questions about the identity fraud environment in New Zealand. The aim was to capture current identity fraud activity and the push and pull factors which impacted upon such activity. The diverse nature of the responses received mirror the diverse nature of identity fraud across industries and across borders, as well as the multiple methods of committing identity fraud offences.

The charts provided in this section relate to four specific questions asked of key informants. While their direct responses have been charted to these four questions, some key informants also expressed related opinions in other parts of the interview. Results will be discussed in the respective sections in which responses were given.

5.1.1 Trends

Key informants were asked: *What trends in identity fraud have emerged in New Zealand?* Of note was that 8 of the 15 respondents stated that identity fraud had increased (refer Figure 9). Mr H (NZP) noted that:

Identity fraud is probably the fastest growing crime on the planet.

Justin Kerr (FSF) similarly responded adding:

The evidence from overseas is that there's a tidal wave approaching. And we would be extraordinarily fortunate to avoid it hitting us.

Thus from both the public and private sector, the increase in identity fraud is a concern.

Four respondents stated that credit card fraud had increased. Mr A (Bank A) stated that there had been:

Mainly a lot of credit cards applications under false names.

Dave Kennedy (NZP) stated that:

Obtaining credit under fictional or genuine identities remains the single biggest area we're aware of.

The financial industry has also been affected by an increase in mortgage fraud. Mr B (DIA) stated:

People are stealing other people's identity to undertake bank fraud such as mortgage fraud. This is a newer type of identity theft. It's more complex and it's probably the complexity that's been developed and used for different purposes, rather than just getting a passport to get into Australia to see the All Blacks.

Four key informants stated that identity fraud was a breeder crime. A breeder crime is a crime that enables another crime to be committed. Mr C (Agency C) stated:

Major organised crime groups previously made most of their money out of drugs, weapons and so on. Now they make more money out of people smuggling, people trafficking, and the enabler of that is identity fraud.

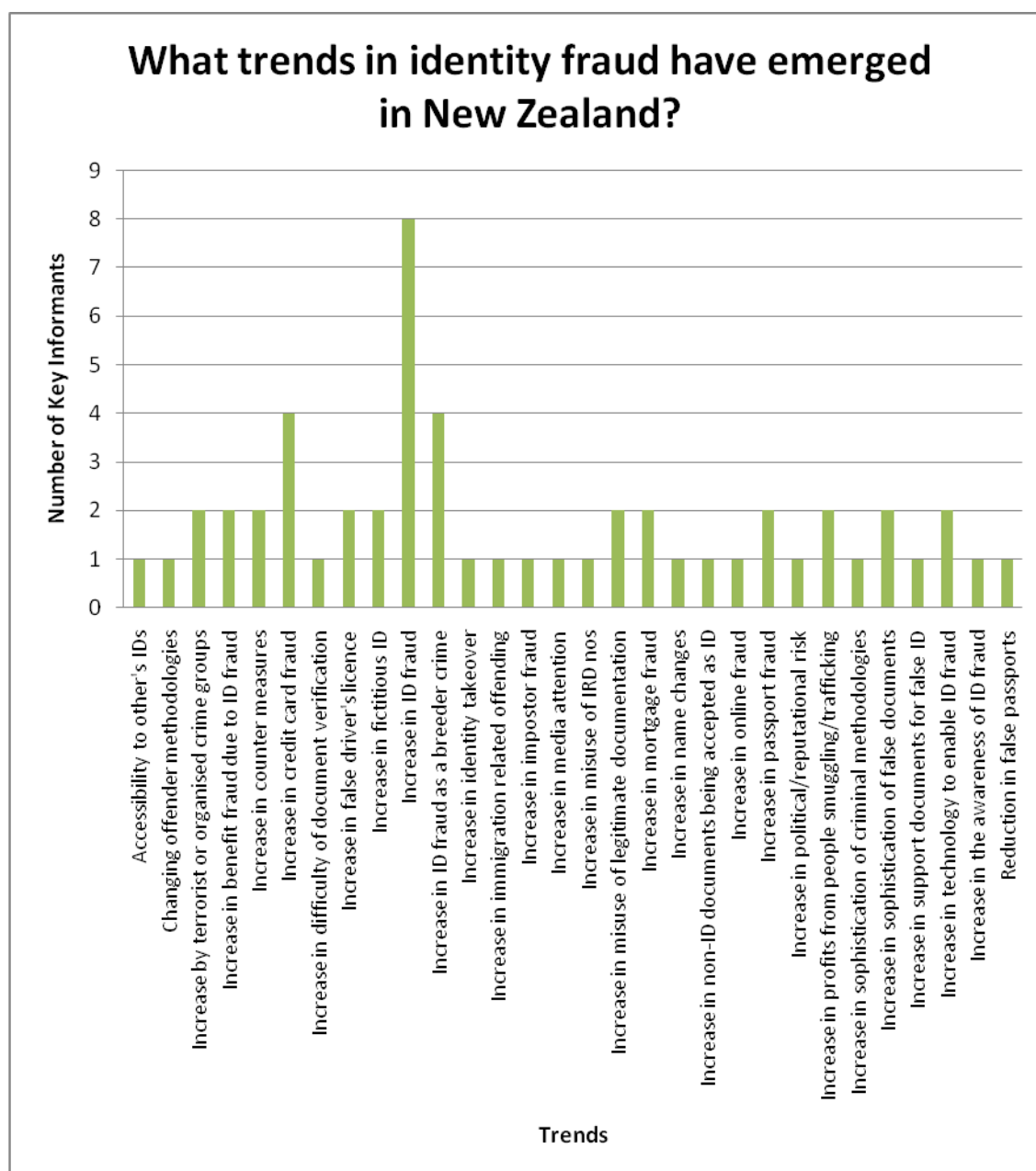


Figure 9: What Trends in Identity Fraud Have Emerged in New Zealand?

From the responses, enablers of identity fraud were:

- The accessibility to other's identities
- An increase in the difficulty of document verification
- An increase in name changes
- An increase in non-identity documents being accepted as ID
- An increase in technology to enable identity fraud

In addition, there were two trends that appear in contradiction of one another, for which further explanation is warranted. They are *Increase in passport fraud* and *Reduction in false passports*. In speaking about passport fraud, Dave Kennedy (NZP) stated:

We're also seeing passport misuse being significant by volume. But that's not just New Zealand passports and that's not just genuinely issued passports, that's also documents that are forged or falsified that purport to be passports, in many cases even photocopies

Mr H (NZP) at the border referred generically to fraudulent passports as "false passports" in saying:

We haven't seen probably more than one or two false passports. I don't know whether that's New Zealand doing the right thing on the international stage and the information getting out to prospective travellers coming to this country. But certainly we're seeing a reduction. Again, that might be due to the new micro bio-data chips, possibly.

This indicates that while there may be a reduction in fraudulent passports being presented at the border, there may be an increase in fraudulent passports being used internally within New Zealand for purposes other than travel.

From the 15 key informants, only 2 key informants stated that they *did not* believe that identity crimes in New Zealand were in line with international trends. Ron Watt (BNZ) was one of these key informants and he stated:

We are fortunate in that we haven't seen nearly the impact of identity crime in New Zealand ... We just haven't the capacity or the legislation to 1) recognise it and 2) deal with it as an identity crisis.

Mr B (DIA) was the second key informant who said:

I feel we're better protected. We have one centralised births, deaths, marriage agency that creates the ability to have a more consistent set of documents which are coming out. That consistency is also carried through to having one police force ... the Passport Office had undertaken a number of years ago some very good procedural changes that put us in a very strong position to really minimise the scope of identity fraud that can occur

in New Zealand. Whereas although numbers of course are greater overseas, the actual scope for what fraud can occur is also greater overseas.

Reasons given for New Zealand being in line with international identity fraud trends included New Zealand not being immune from cyber-crime – but perhaps being a few years behind in other areas; increasing evidence of credit card fraud as a pointer; ongoing development needed for Government operational capabilities to go with identity frameworks; similar movement of inadmissible persons across international borders; the manufacture of counterfeit New Zealand passports overseas; passport fraud being present in New Zealand.

Alan Thompson (NZCS) commented:

We may be slightly worse than anywhere else but without any figures it's very difficult but we're seeing the constant supply of misused or misrepresented identities coming through at the border, for use in New Zealand or to facilitate entry to New Zealand or exit from New Zealand to somewhere where people shouldn't be going.

Similar sentiments were echoed by Jim Furneaux (NZTA) who stated in relation to New Zealand trends:

We don't really have any proper systems to measure this, so while we think it might be a trend it's only what we're seeing. What's actually happening we don't know.

Mr A (Bank A) similarly responded:

There's no really recorded, well recorded stats around it.

The next section is going to examine the issues in identity fraud in New Zealand.

5.1.2 Issues

Key informants were asked: *What do you think the issues are surrounding identity fraud in New Zealand?* Opinion among the 15 key informants was spread rather evenly on this question as can be seen from Figure 10 below:

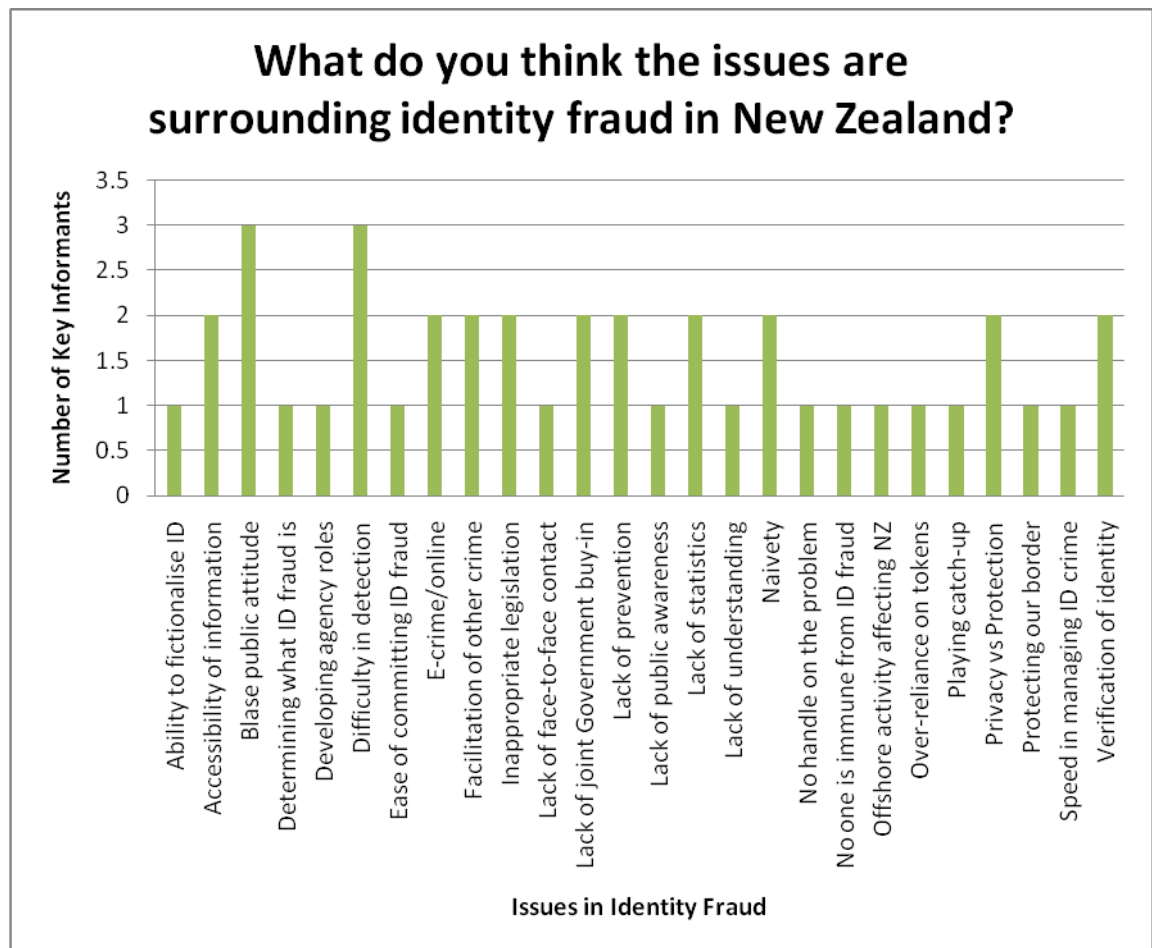


Figure 10: What Do You Think the Issues are Surrounding Identity Fraud in New Zealand?

New Zealand's relatively isolated geographic location is perhaps a contributor to one of the highest rating issues in identity fraud: *Blasé public attitude*. Paul Hurrell from (IAG) stated:

Everybody's just so lax. It's just complacency's the hardest fight of the lot.

This issue was closely related to *Naivety* which, in the eyes of the rest of the world, can make us an easy target. Ms F (Agency C) commented:

New Zealanders they believe are sort of naive because we are at the other end of the world. And therefore they believe that it is actually an easy target to come down here. We have lots of issues with, obviously, Nigerians using South African passports, posing as South African nationals coming to New Zealand.

While it is unlikely that identity fraud is the only arena in which New Zealanders think 'It won't happen here ... it won't happen to me', public vigilance is imperative given

that the other highest category was *Difficulty in detection*. Kate Antonievich (DIA) advised that the way in which society now operates makes it more difficult to detect identity fraud:

The anonymity that we now operate under through the use of online channels ... when I go into bank branches no-one knows who I am, when I go to the library no-one knows who I am. Makes it much easier for me to adopt a false identity or to adopt someone else's. And that in turn makes it very difficult, much more difficult, to detect or prevent those types of crime.

Detection is further compounded if identity fraud is used to perpetuate another crime (as mentioned in the previous section). Ms G (DIA) stated:

People need to understand that identity fraud or identity crime is usually a facilitator and enabler for many other offences and activities.

Furthermore, from the Government's perspective Alan Thompson (NZCS) said:

We need to know who is in New Zealand – that's a sovereignty issue ... Customs being responsible for sovereignty of New Zealand through the protection of its border. So knowing who's here, knowing that they're not going to do a wrong, perpetuate a mischief. Because you can hide criminal activity behind a false identity.

The high speed in which an identity fraud offence can occur makes real-time detection extremely difficult. The ability to catch an offender is often stymied by the inability to verify his or her identity. Dave Kennedy from the New Zealand Police advised:

The ability to fictionalise ID is definitely an issue in New Zealand. And the inability of Government and more so the private sector to ascertain whether or not an ID actually exists or not.

The private sector is even more disadvantaged by not being able to access identity information held by the New Zealand Government due to provisions in the *Privacy Act 1993*. Verification and further investigation into identity fraud becomes even more difficult when the offences against New Zealand identities occur in other jurisdictions.

Andrea Gray (DIA) commented:

It may not be identity fraud in New Zealand but it may be affecting New Zealand. And so there might be things happening offshore, either with New Zealander's identities, or things that happen offshore which can then be brought to New Zealand to perpetrate crime.

Thus, New Zealand must rely on foreign agencies to pursue any prosecution action which may or may not happen. In addition, it is rather difficult to detect for instance, the manufacture of counterfeit New Zealand passports in offshore locations, without foreign governments advising of such activity.

Issues in identity fraud also impact upon government programmes aiming to manage the identity fraud risk. Mr C (Agency C) stated:

There are very strong policy frameworks emerging around managing evidence of identity. As recent cases in the media have highlighted we need to move a lot faster to develop some very practical capabilities across government to manage identity crime, we are probably not as mature as we need to be in this regard.

However, without a quantitative figure as to the impact of identity fraud in New Zealand, these Government programmes cannot categorically address the issues at play. Mr A (Bank A) said:

The New Zealand Police don't record specific stats around identity fraud so the New Zealand Government's got no idea how much it's costing the New Zealand tax payer. Australia I think they talk about a billion dollars a year. So yeah we got no real handle on it in New Zealand.

The lack of statistics and reporting around identity fraud in New Zealand can perhaps be attributed to the lack of specific identity fraud or identity crimes legislation. Jim Furneaux (NZTA) stated that in relation to issues in identity fraud:

Inappropriate legislation is the main one – certainly for us. The fact that we don't have any real legislation that helps us ... It needs to have specific clauses, subsections in there that relate to types of offending that are prohibited and the use of documents.

Despite the systems that are currently in place in New Zealand (these will be discussed in detail in the next chapter of findings), it is not difficult in some instances to commit identity fraud. Mr D (Agency D) commented:

Those issues are how jolly easy it is for people to commit identity fraud. And I can think of a case here in New Zealand where a guy, a New Zealander, searched the Internet, he was living in the States ... He applied and got a birth certificate, which was around the same age as his child. Applied for a New Zealand passport and travelled with the child that he had taken from the States to New Zealand ... And as result of an extensive interview here in New Zealand we were able to establish how easy it was for him over the Internet to obtain that information.

This leads to the next section which details the main threats in identity fraud in New Zealand.

5.1.3 Main Threats

Key informants were asked: *Where do you perceive that the main threat of identity fraud comes from in New Zealand?* This question resulted in a range of 19 response categories (refer Figure 11 on the next page). In terms of human entities, the main threats were from the following groups:

- Asian community
- Foreigners bringing their criminal methodologies
- Impostors with genuine documents
- Isolated criminal entities
- Organised crime
- People wanting to gain financial advantage
- People wanting to use false ID for a specific purpose
- People with personal life issues
- Student community.

Of the human threats, *Organised crime* was the highest scoring category with five key informants stating that they were a main threat. Dave Kennedy (NZP) further identified the organised crime groups that he believed were a threat:

I mean things like Asian organised crime, West African organised crime and Eastern European organised crime. Those three very generally labelled crime classes are professionals and well-experienced at this kind of activity.

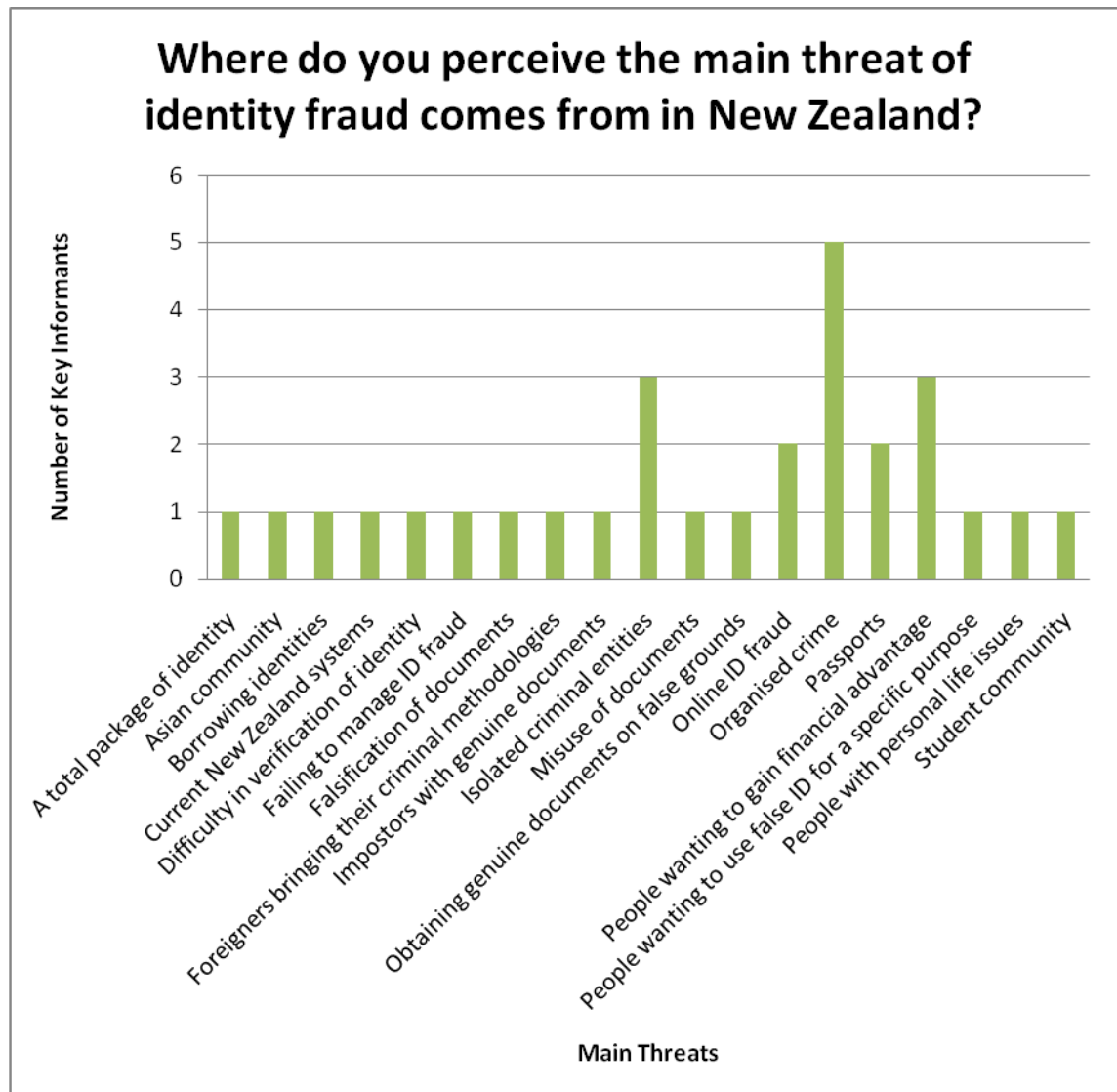


Figure 11: Where Do You Perceive the Main Threat of Identity Fraud Comes from in New Zealand?

New Zealand home-grown organised crime groups were also mentioned by Mr D from Agency D who said:

I can just think back to a gang in Auckland that were purposely stealing from letter boxes where they must have had a contact with the postal

service or whatever and obtaining credit cards, identity cards, and committing frauds with those – organised crime, gangs.

The tied second highest ranking category was that for *Isolated criminal entities* with three key informants mentioning this group. Kate Antonievich (DIA) nominated Wayne Thomas Patterson – the man who obtained 123 identities to fraudulently obtain \$3,414,425 of benefits from the Ministry of Social Development as one of New Zealand's most high profile fraud cases and said:

I don't sort of know where it's going to go really ... whether individuals will end up being the bigger profit for us than organised crime.

Nonetheless, *People wanting to gain financial advantage* was the other second tied category, reinforcing the monetary motivation for individuals such as Wayne Patterson to commit identity fraud. Jim Furneaux (NZTA) commented:

By and large I think most of it really somewhere along the line is related to somebody trying to gain fraudulent advantage, rather than just simply changing their identity. Almost all of it comes back to somewhere to somebody doing something with money.

The financial motivation of identity fraudsters places a great strain on private sector businesses such as financial institutions and insurance companies, who rely on identity documents in their daily business. However, these documents also pose a large threat.

Ron Watt (BNZ) stated in relation to threats in New Zealand:

The first and most prevalent one to date is the falsification of records and documents and indeed the creation of records and documents. I'm talking about birth certificates, driver's licences and those sorts of things. People think they're hard, particularly a driver's licence and a passport to copy. They're not. They're easy.

Impostors on genuine documents pose a further threat because even if document verification is conducted, records will show that a document has been legitimately issued but it will not necessarily prove the document is in the hands of an impostor. In society, there are some people who can easily resemble other people and with time

pressures to meet service standards and the inability of businesses to have access to automatic facial mapping technology, detecting an impostor can be inherently difficult.

Justin Kerr (FSF) said that in New Zealand the main threats came from two sources:

One is the recreation of documents that appear to be genuine which establish, or appear to establish that the identity of the person who is presenting in a situation seeking a loan is someone they're not. The other would be borrowing identity (sic) and altering a few elements so that enquiry would show that the person is a real person and that most things stack up. But they aren't, they are not actually that person.

Furthermore, the deterrents in New Zealand for committing an identity fraud offence do not appear to outweigh the benefits of committing the identity fraud offence. Mr A (Bank A) commented:

Criminals have now realised that identity fraud, you can make big returns for very little risk. The chances of getting caught are very remote. And if you do get caught it's well, you know the penalties are very light.

Sadly, current and legitimate systems in New Zealand can even assist identity fraudsters in their ambitions. Paul Hurrell (IAG) stated that he believed a main threat came:

From people who are coming in from overseas and bringing in different ways of doing things that we're not used to doing. And that the New Zealand public in general don't believe that someone would do ... they can have numerous identities within a very short space of time just by using our systems that we've got available now.

Paul Hurrell was referring to the ability of foreign nationals in New Zealand being allowed to change their name by statutory declaration through the Births, Deaths and Marriages unit, Department of Internal Affairs¹⁹. The form merely requires an individual to declare their birth name and what they would like to change their name to, without even asking if they have been known by any other names since their birth name. While one would believe that these people would cease to use their previous

¹⁹ The *BDMRR Act* came into force on 25 January, 2009 and an individual must now be a New Zealand permanent resident or New Zealand citizen to change their name in New Zealand.

names and only use their new name, this is not always the case and there is no legislation to enforce this otherwise. Moreover, once their name is changed, agencies and private sector businesses can be duped by a non-declaration of their previous names (which may reveal a criminal past).

A legitimate name change in New Zealand can contribute to what Mr H (NZP) calls a “total package of identity”. The threat from such a package is that an individual can have a back-up identity document to support any other fraudulent ID provided to an organisation. Mr H states:

From our experience, the internal identity theft, if you like appears to be mirrored by the external and that's again from the Asian community. We're noticing that within the student community we're seeing identity fraud that's actually produced here and also overseas and either sent in via cargo or mail centres. There's certainly evidence that we've come across of on-line identity scams ... involving Chinese students. Not just for producing degree documents but things like driver's licences and identity cards ... I think the main ... threat if you like is the production of a total package of identity. So starting off with the classic 'Day of the Jackal' cases of obtaining deceased children's birth certificates, I just don't think they're as common as we expect. I think the classics are obtaining lines of credit, credit cards, getting driver's licences and then building up a package of ID. I think that's where the threat comes from.

The types of documents that are open to abuse in New Zealand are discussed in the next section.

5.1.4 Abused Documents

Key informants were asked the question: *What documents of identity are mainly abused in New Zealand?* Birth certificates were the most mentioned document with 10 key informants stating that they were abused, followed by 9 key informants who mentioned both *Passports* and *Driver's licences* (refer Figure 12 on the next page). While one may argue that a birth certificate is merely a certification that an individual was born and a driver's licence is nothing more than a permit that allows one to drive,

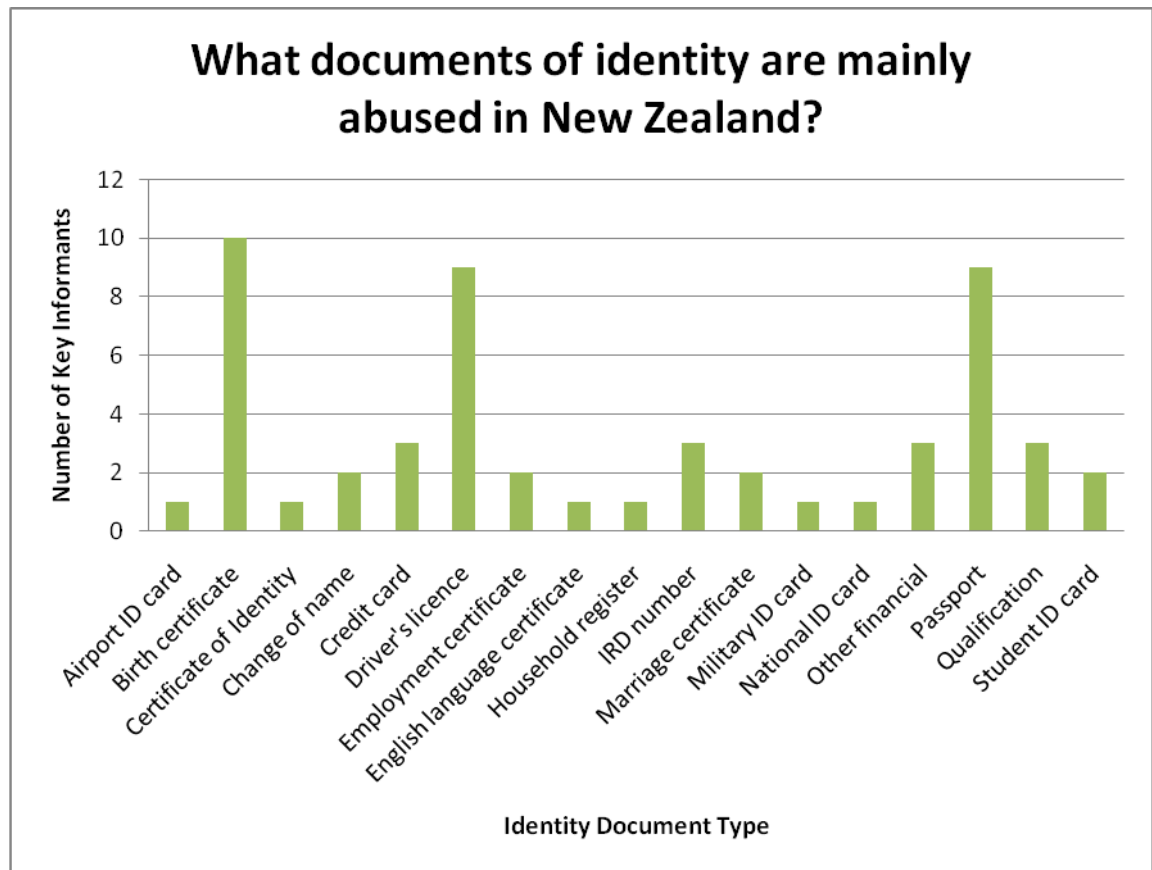
they are both commonly accepted documents of identity or supportive documents of identity in New Zealand. When asked the question regarding document abuse Mr C (Agency C) stated:

I think it's the full range. Well it depends on your definition of a document of identity. You know some people would say a birth certificate. In the Immigration context it's just about every single document that is or purports to be an evidence or a proxy of identity – from passports, household registers, birth certificates, driving licences, military ID cards, national ID cards. And then the second level of documentation which can be evidence of use of identity in the community: marriage certificates, employment certificates, English language attesting certificates – and so on. All are vulnerable and have been fabricated.

Birth certificates of New Zealand born individuals are openly available for purchase through Births, Deaths and Marriages, Department of Internal Affairs. This means that anyone can purchase anybody else's birth certificate – a legitimate document issued by the New Zealand Government. While there are few organisations that would accept a birth certificate per se as evidence of identity, they are commonly used as supporting documentation – both in New Zealand and overseas. Jim Furneaux (NZTA) expressed concern about the ability to forge or counterfeit a birth certificate:

You can simply run those off, find some paper that more or less matches and run them off. I mean with photo-shop tools and that type of thing these days you can run off anything you like, pretty much.

Foreign birth certificates can prove even more problematic with fewer avenues of verification for New Zealand based businesses and sometimes even the public sector.



NOTE: *Other financial* includes mortgages, cheques, bearer bonds, credit applications, letters of credit

Figure 12: What Documents of Identity are Mainly Abused in New Zealand?

Passports are New Zealand's most secure document due to the security features and the strict procedures around its issuance. Nonetheless, instances of false passports, forged passports and counterfeit passports do occur for a number of reasons, for example, the availability to counterfeiters of improving technology or the presence of an older passport with fewer or less robust security features. Additionally, as previously mentioned, there is also the risk of an impostor using a genuine document. While the technology used in securing the New Zealand passport is good and in line with International Civil Aviation Organisation (ICAO) guidelines, this cannot be said of passports from all overseas countries. Both the New Zealand private and public sectors alike rely on the veracity of the passport presented and factors such as corruption or poor technology in other countries may impact upon the integrity of the passport. Andrea Gray (DIA) commented in relation to the abuse of documents in New Zealand:

Passports can be by being photocopied and being accepted as photocopies ... As organisations like ours use more data-based services then the possibilities of those documents being abused, certainly for our services at least, become much less.

This is due to the fact that the Department of Internal Affairs administers the New Zealand passport database and has access to source documents for New Zealanders. However, this does not negate the issues outlined on the previous page.

Driver's licences are acceptable forms of identity in the private sector. In New Zealand, with the absence of a national identity card, the driver's licence has become a 'de-facto' identity document as it is the only document on which is it compulsory to have a photo of the holder. Even Jim Furneaux, the Manager of Driver Licensing acknowledged that in terms of abused documents:

Driver's Licence is right up there.

Justin Kerr (FSF) advised of the problems with driver's licences in the finance industry:

The more common document that would be used across our membership would be driver's licences. There are more limited instances of those having been forged. What's more common is for individuals to obtain more than one copy of the driver's licence in different names ... somebody has obtained a licence in a name, in a slightly different format name than their name. They may have two of the licences or three but that's not uncommon.

The ease with which one can change one's name in New Zealand by statutory declaration was also cause for alarm for two of the major banks. Ron Watt (BNZ) advised:

Another form of identity theft probably is the name change – legitimately changing a name and creating a new identity for yourself, which is just so easy in this country to do. It's just amazing. In fact we've had one case recently where an individual changed their name by deed poll, legitimately, seven times and all within a matter of 12 months. And you know each time it was to commit a fraud, a criminal activity.

Mr A (Bank A) also voiced his concerns:

The biggest problem we've got here is the fact that anyone can go in and change their name by deed poll. And we've had one instance I think where they changed their name seven times in a day. You do not have to be a New Zealand citizen to go in and change by deed poll. You can be a Vietnamese citizen get off the plane, go straight round to the Court and change your name by deed poll²⁰. And it has happened. So once you've done that of course you can get a pass, you can get a driver's licence immediately issued in those improvised names. And away you go. You can then apply for credit cards and whatever under a new name. And instantly change your name again so you won't be recorded on Baycorp 'til somebody links all of your identities.

The threat of document abuse was philosophically summed up by Mr H (NZP), who stated:

My experience with identity theft, any document is susceptible to alteration.

5.2 SYSTEMS ISSUES

In this section, key informants were asked about the impacts of identity fraud in their respective organisations; what documents gave them cause for concern; how they currently verify identity, their best practice parameters and the consequences for ineffective identity verification. In addition, they were questioned as to how they shared information – both domestically and internationally; and what systems and projects their organisations had set in place in order to minimise identity fraud. The other issues discussed were the barriers they faced in combating identity crimes as well as identity fraud costs and statistics.

5.2.1 Identity Crimes and Documents

In terms of the types of identity crimes that effect organisations, both key informants from the two banks stipulated that mortgage fraud was an issue. Ron Watt (BNZ) stated:

²⁰ Since the *BDMRR Act* came into force on 25 January 2009, it is no longer possible for a non-permanent resident of New Zealand to change their name by Statutory Declaration (formerly known as by Deed Poll).

Mortgage scams, loans, creating or taking the identity of a person and using it to purchase property in their name and then selling that property before the fraud or the identity creation has been detected.

Credit card fraud was also an issue, as was the obtaining of finance in the private sector. Justin Kerr (FSF) advised that if presented with a false identity, both the finance company and the retailer would 'lose' as they would be unable to trace the offender. The fourth key informant from the private sector, Paul Hurrell (IAG), cited problems with the identity fraud of internal staff members as well as insurance customers who commit identity fraud to cover-up past declined policies. Further motivation to commit identity fraud was due to the fact that:

Insurance policies do not generally require verification of the customer's actual true identity and they can use this to try to hide assets from government departments etc..

Four of the key informants from the public sector advised that identity fraud and/or identity documents were a breeder for other crimes. Andrea Gray (DIA) stated:

The systems issues that affect DIA most I think are the fact that across the board documents are used in a range of different situations and they can build on one another in terms of forming a view about an identity.

Mr C (Agency C) said that his organisation was concerned about the management of false identities that will impact further in other agencies or the financial sector:

Immigration's got to manage identity fraud as a breeder, or a pre-cursor, for any number of adverse outcomes that could affect other people ... So it's quite a broad challenge. And if you don't get identity right, you can't get anything else right. You can't reliably establish a criminal history, medical history, employment history, qualifications, the works.

The consequences for getting an identity wrong could be catastrophic with Mr D (Agency D) citing identity fraud as being an enabler for terrorism and people smuggling or human trafficking. Alan Thompson (NZCS) stated:

Any misrepresentation of identity across the border destroys the transaction ... so if you haven't got the person you think you have in front of you then

that's an issue. And that transfers back to all those other things, transnational organised crime ...

Some form of fraudulent documentation was an issue for six of the key informants with two of them mentioning driver's licences and another two mentioning fraudulent passports as being problematic for their organisations. In respect of driver licensing, Jim Furneaux (NZTA) said that driver licensing was used in two respects in relation to identity fraud: (1) foreign nationals using fraudulent overseas licences in New Zealand or foreign nationals coming into New Zealand under a false identity and later asking for a change in their details once they have claimed refugee status; (2) New Zealand driver's licences being used as a supporting identity document or as a breeder document in order to commit another type of fraud.

When the key informants were asked what documents of identity were commonly presented to their organisations that gave cause for concern, the answers given reflected the subjective nature of what actually constitutes a 'document of identity'. Driver's licences and passports scored the highest with eight key informants each stating that these documents gave their organisation cause for concern. In respect of passports and systems, Ms F (Agency C) said that both foreign and New Zealand passports were of concern but:

With the introduction of the NZAPP and RMAL system, anyone who reports their New Zealand passport lost or stolen and is heading our way or to Australia or the US, it puts out a regional alert, identifies to that economy that the passport has been lost or stolen. However, it doesn't affect if the person is travelling to another economy outside of those three countries.

This means that the system is limited to travel to New Zealand, Australia and the United States of America, but the alert system will not prevent a lost or stolen passport being used in say Zimbabwe or for non-travel use in any country – such as using the passport for identity purposes to obtain credit.

Five key informants stated that overseas documents and birth certificates were a problem for their organisations. The issue with overseas issued documentation largely revolved around the integrity of the document from the country it was issued in and the difficulty in having a document verified. Mr C (Agency C) stated:

It's important to get the right understanding of the inherent risk in the document itself or the identity associated with the document – what are the government institutions like in that country? Are those passports able to be obtained fraudulently through corruption etc.? In some countries, corruption in the passport agencies means people have legitimate documents and if you attempt to verify the document with the issuing government you'll get told 'Yes that's a real passport'. But the person's still not who they say they are because the passport was issued corruptly. We've seen that with the South African passport big time at the moment. For four hundred dollars, you can, anyone from anywhere, can go to South Africa and get a real South African passport that will be authenticated by the authorities when we check back with the SA Government.

The private sector in New Zealand faces a further challenge in the verification of documents in New Zealand due to restrictions under the *Privacy Act 1993* so overseas verification becomes even more problematic. Paul Hurrell (IAG) advised:

In relation to staff it's birth certificates or marriage certificates, those sorts of things, so that we can't find out the true identity of the person we're actually employing. Especially when they come from overseas. It's just impossible to make those sorts of enquiries.

Other documents that gave organisations cause for concern were receipts, bank cards, certificates of identity, bank statements and student identity cards. While only one key informant mentioned a student identity card, the comment was rather alarming. Mr H (NZP) stated:

You can go onto Phantasm.com and get yourself a student ID. Cost you about \$5. In fact I had a Chinese student who was at Otago earlier this year who produced an entire Hong Kong police identity. Warrant cards, IDs. He had it in the same wallet as his student ID. He also had a Hong Kong police uniform which he was wearing down in Otago. And we think he was using it to extort monies from young Hong Kong students.

This example demonstrates the lengths that people will go to and the potential damage that can be caused by a fraudulent document of identity - hence the need for effective channels of identity verification.

5.2.2 Identity Verification

The ability to verify an individual's identity is core to the identity fraud system. Key informants were firstly asked how their organisation verified identity; secondly, what concerns they had with their organisation's identity verification procedures; thirdly, what the consequences were to their organisation for ineffective identity verification and finally, whether their organisation had best practice parameters around identity verification.

In relation to how their organisations verified an identity, six of the key informants stated that they verified identity with Government departments in New Zealand. Public sector agencies have the ability to share private information through vehicles such as Memorandums of Understandings and under Principle 11(e)(i) of the *Privacy Act 1993* where:

Non-compliance is necessary –

(i) To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences

However, the private sector is limited in their ability to obtain personal information and thus limited in their ability to verify identity. Two of the key informants who provided this answer were from the private sector and despite saying that they attempted to verify identity through public sector agencies, they both expressed concern at the problematic nature of identity verification with the public sector:

There's no sort of document sharing for the register of births and deaths that birth certificates aren't genuine. Or driver's licences were issued to Mr A so and so or the like. Mr A (Bank A)

Sometimes we can get identification verified and sometimes we can't. It all points to the lack of proper identification type processes in this country, quite frankly. Ron Watt (BNZ)

Nonetheless, while the private sector faces more challenges than the public sector due to the *Privacy Act 1993*, the public sector even faces opposition within its own ranks. As previously mentioned, the Inland Revenue Department is unable to share information with other public sector agencies due to the secrecy provisions in the *Tax Administration Act 1994* – even if the individual in question gives authority for another agency to conduct checks with the IRD. Births, Deaths and Marriages at the Department of Internal Affairs will give the information but only if it is paid for and applied for in the standard manner. This causes difficulties with the likes of agency investigations when information may be needed urgently. Mr H (NZP) advised of a further challenge that his organisation faces in relation to driver's licence verification:

You could actually get a photograph up on our system. Sadly, we can't access LTNZ photographs which is a persistent pain.

Three of the key informants from public sector agencies commented that they make good use of overseas verification. Mr C (Agency C) commented:

I think the first line of defence is that we've got some really good people out in the embassies overseas who speak the languages, know the accents, know what the documents look like, know how to authenticate documents in non-traditional ways. We do site visits in high risk markets. So we'll go to villages in India, and factories in China, and restaurants in Bangkok. And we'll do a lot of checking. And it's like the social footprint. When you have an environment where you can't have a high degree of confidence in documentation you go out and you look at the context of that person.

However, overseas verification of identity with government agencies proves impossible for the private sector. Ron Watt (BNZ) said:

Overseas passports; it is very difficult for us. Generally we would go back to the other bank and the overseas bank, and just ask if they know the person. We wouldn't, or couldn't, go to the overseas government department that issued them. They won't give us that sort of information.

While overseas government verification is difficult for banks, they have international obligations to identify any potential terrorists as part of their systems. Ron Watt (BNZ) further advised:

Any international transfer that comes in or out of this country via BNZ is verified by the Bank against the OFAC²¹ list (European list) and also the New Zealand Prime Minister's list. So any money that's particularly going out of the country or even coming in, the identity of the beneficiary or the remitters of those funds, is checked against those lists. We also, every day, check our own database e.g. new accounts opened up.

Overall, key informants advised of a number of ways in which they verified identity. These included body markings, hospital records, credit agency checks, a tiered system of identity documentary evidence, verification with witnesses, fingerprints, criminal history checks, document examination, data comparisons. However, three of the key informants stated that their organisations had no formal systems in place to verify identities. It is a concern that in New Zealand, a driver's licence is a commonly presented and accepted form of identification, yet there is little verification as part of the system of granting a driver's licence to an individual. Jim Furneaux (NZTA) remarked in relation to how his agency verified an identity:

We don't. We can if we have an issue, but if you're talking about 99.9 percent of people who just rock on in, it's you produce your certificate of identity, or your acceptable form of identity, evidence of identity, and your evidence of address. Now both of those could be forged. We have no way of checking anything. We have no online system with Births, Deaths and Marriages (BDM) for argument's sake. And we do not check to see whether, somebody who's supposedly come in from overseas, has actually entered the

²¹ OFAC is an acronym for Office of Foreign Assets Control, part of the United States Department of the Treasury. OFAC "administers and enforces economic and trade sanctions based on US foreign policy and national security goals against targeted foreign countries and regimes, terrorists, international narcotics traffickers, those engaged in activities related to the proliferation of mass destruction, and other threats to the national security, foreign policy or economy of the United States." (United States Department of the Treasury, n.d.).

country in that name. And in neither case, whether they're New Zealand born or born overseas, do we make sure that they're still in the country. Which is, I think, a factor that most people forget. You can verify that something exists, but you don't necessarily know that person's still in this place. So yeah, so it seems to me that if we were going to verify it, we would need to be with BDM, Immigration, Internal Affairs and probably Customs to make sure that people were, or whoever it is, that we can get the data off with the least number of checks.

When key informants were asked what their concerns were in relation to their organisation's identity verification procedures, only two key informants advised that they did not have many concerns (one key informant withdrew their answer to this question). Mr A (Bank A) advised:

I think we're as strict as we can be without you know getting out of line with our competitors. If you make it too hard for people over the counter they'll just go somewhere else. And of course we don't want that.

The other key informant who was positive about their organisations identity verification systems was Andrea Gray (DIA) who responded:

Very few in comparison to those that I might have about other agencies. In that, we are well-practised, we think about it a lot, and we understand some things about identity. Having said that, you can't always expect to be perfect. And DIA's really in a sense, will be staking out the territory to be a lead in the quality of process and the thinking behind that, so it'd be terrible if we were saying something different.

In terms of concerns that key informants had with their organisation's identity verification procedures, they ranged in summary as follows:

- Need for more human resources
- Increasingly arduous legislative requirements
- We're going to miss something
- Impact on organisational credibility
- Lack of biometrics
- Citizenship processes

- Lack of consistency
- Risk profiles
- Reliance on bio data alone
- No base for establishing identity in New Zealand
- Fingerprint processes
- Lack of custodian in New Zealand for identity processes
- Lack of online verification
- Human oversights
- Lack of staff training
- No basic training standard
- There is no foolproof system
- Tightening up of procedures needed.

The above list of concerns reflects the varying systems and their associated activities across organisations and agencies in New Zealand. The highest scoring category was the lack of staff training. Three key informants expressed this as a concern in verifying identity. Their comments are as follows:

In terms of identity verification, I don't think there's a basic training standard. Mr H (NZP)

Not a lot of the staff are trained in it. Training is quite an issue. We only seem to have really one to two people that have extensive knowledge of document examination techniques and knowledge of various documents from around the world as well as our own document. Ms F (Agency C)

The skill of the frontline officers ... So there's a risk there because of the calibre of the employee at that particular point in the process. Alan Thompson (NZCS)

The second equal highest area of concern was the 'Lack of biometrics' used in the identity verification system in New Zealand with two key informants mentioning this as

an area of concern. While facial recognition technology has been used by some agencies in New Zealand, biometric databases (with the exception of individual's photos) have not traditionally formed part of the identity system. The sole reliance on bio data information is a risk for both the private and public sectors where the misuse of another person's details is not out of the ordinary. Mr C (Agency C) provided the following comment:

The use of traditional information: names, dates of birth, passport numbers – it's just got no efficacy in managing identity crime in a world where people are deported from New Zealand, go and get a new passport, a legitimate passport with a different name and date of birth and come back. We really have to implement a robust biometric-based identity management capability to take the next step in managing identity fraud ... you can throw thousands and thousands of hours and time in verifying every single application, every single document – but if you're using biometrics to automatically verify identity, particularly people who you've dealt with in the past under another identity, it's just so much more efficient and reliable using biometrics.

The other area of concern that shared the second equal rating was 'Increasing legislative requirements'. The two key informants who cited this concern in identity verification in their organisation were from the private sector. With an international move to curb the incidence of identity fraud, there is international pressure for countries such as New Zealand to introduce legislation that places the onus of identity related matters on to organisations such as banks. The two key informants stated:

Increasing legislative requirements have been placed on lenders to not only do what they think is needed but to meet international standards under the FATF protocols. Justin Kerr (FSF)

It has been a real responsibility and liability placed around banks to make sure we don't deal with a terrorist or a suspect entity or party, and you know, in my view, it has actually been quite unfair. All of this has just been thrown at the banking industry and said 'you do this' and we do it ... but if you do send money to an overseas destination, a banned country for example, and it's picked up by the American authorities, they will run you through the hoops, they will investigate and levy a fine on you for doing that particular transaction. Ron Watt (BNZ)

Legislative issues in New Zealand will be discussed further in section 4.0 of these findings.

When key informants were asked what the consequences were to their organisation and the public for ineffective identity verification, 9 of the 14 key informants who responded to these two questions stated that their organisation would face a 'Loss of reputation, credibility or integrity' (see Figure 13 which details only those consequences where there were two responses or more). It impacts upon the private and public sectors alike and this consequence per se is fraught with its own set of consequences. For example, in relation to the 'International penalties' consequence, if multiple failures in identity verification brought the integrity of the New Zealand passport system into question, this could cause countries such as the United States of America to cease New Zealand's visa free status, causing further cost to members of the public who wished to travel there by having to apply for a visa. The following are two comments from the public and private sectors:

The consequences to us as an organisation are a huge loss of reputation and then a whole lot more – sort of questioning of our general ability to carry out the functions we're responsible for. And that then tends to you know end up with reviews and changes to the way we do things and so on. Kate Antonievich (DIA)

The public perception that your bank's not safe. Or you're slack. So there's an adversary public reaction to banking with you. That if your criteria or procedures are bad. Or how safe is their money. That of course is a public thing, shareholder value. Mr A (Bank A)

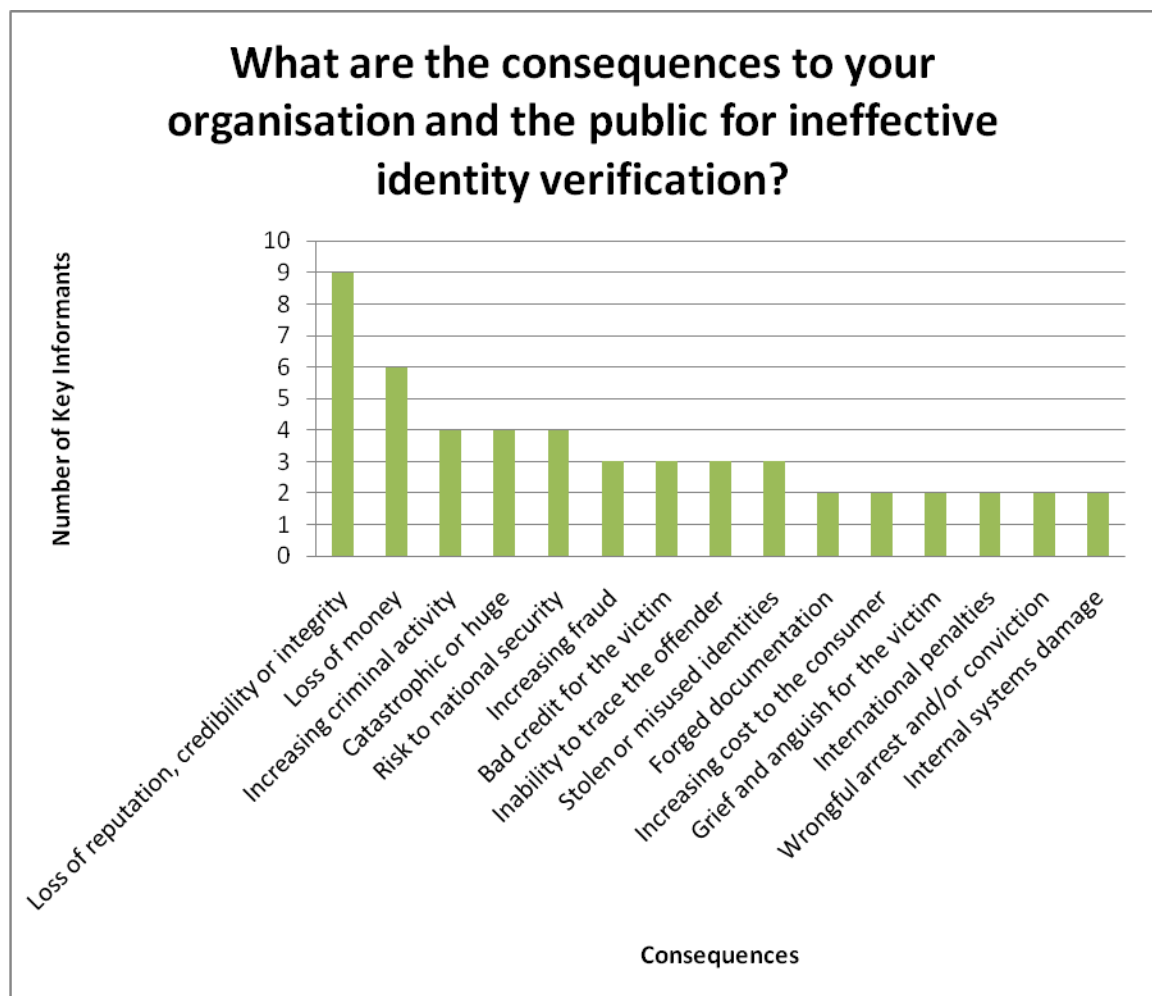


Figure 13: What are the Consequences to Your Organisation and the Public for Ineffective Identity Verification?

Six of the 14 key informants cited ‘Loss of money’ as a consequence for their organisation. This can also lead to it being a consequence for the public with Paul Hurrell (IAG) commenting that a failure in identity verification could lead to “paying out on claims that weren’t legitimate claims”, subsequently leading to a loss of income for shareholders. No doubt a loss of income to an organisation is strongly linked to ‘Increasing cost to the consumer’ which was mentioned by two key informants. Jim Furneaux (NZTA) advised that any driver’s licence issued to a fraudulent individual by his organisation enables “people to commit fraud. Which then starts hurting everybody, your insurance rates go up, your bank rates go up, all that kind of stuff”.

The consequence of ineffective identity verification for four of the key informants organisations would be 'Catastrophic or huge' with four key informants stating that it would lead to an 'Increasing criminal activity' or cause a 'Risk to national security'. Ms F (Agency C) said:

We would end up with persons who pose a threat to New Zealand's borders, i.e. potential terrorists, gangs of organised crime and we'd end up in Court. We could be prosecuted. It has huge ramifications.

As discussed earlier, identity fraud is a breeder crime, hence its ability to increase criminal activity in the event of an identity verification failure. This leads to other consequences listed on Figure 13 for any victims of identity fraud including bad credit, grief and anguish, wrong arrest and/or conviction. Traditionally, these consequences to victims are not able to be solved easily with innocent individuals having to prove to the likes of authorities and/or financial institutions that it was not them that committed an offence or applied for finance. Consequently, the grief and anguish caused to victims can be ongoing.

Despite only receiving a mention from one key informant each, the following consequences to the public and organisations resulting from ineffective identity verification are no less important:

- Penalties for organisations from legislation
- Unlicensed drivers on the road
- Accelerated loan processes
- Increasing questioning of consumers
- Failure to meet Government outcomes
- Criminal and civil liability
- Loss of income for shareholders

- Prosecution against the organisation
- New Zealand becomes a known easy target for criminals
- Public safety
- Lack of confidence by public in Government
- Inability to trust or use Government documents
- Damage to the community
- Degradation of sovereignty.

Finally, on the topic of identity verification, key informants were asked whether their organisations had any best practice parameters around identity verification. Some key informants sought this explanation as to what best practice meant and this was explained as being any policies or procedures that were in place as part of a system in their organisation. As can be seen from Figure 14 below, eight key informants advised that they did, zero key informants said that they did not, four key informants advised that they partially did and two key informants were unsure. One key informant deleted their response to this question.

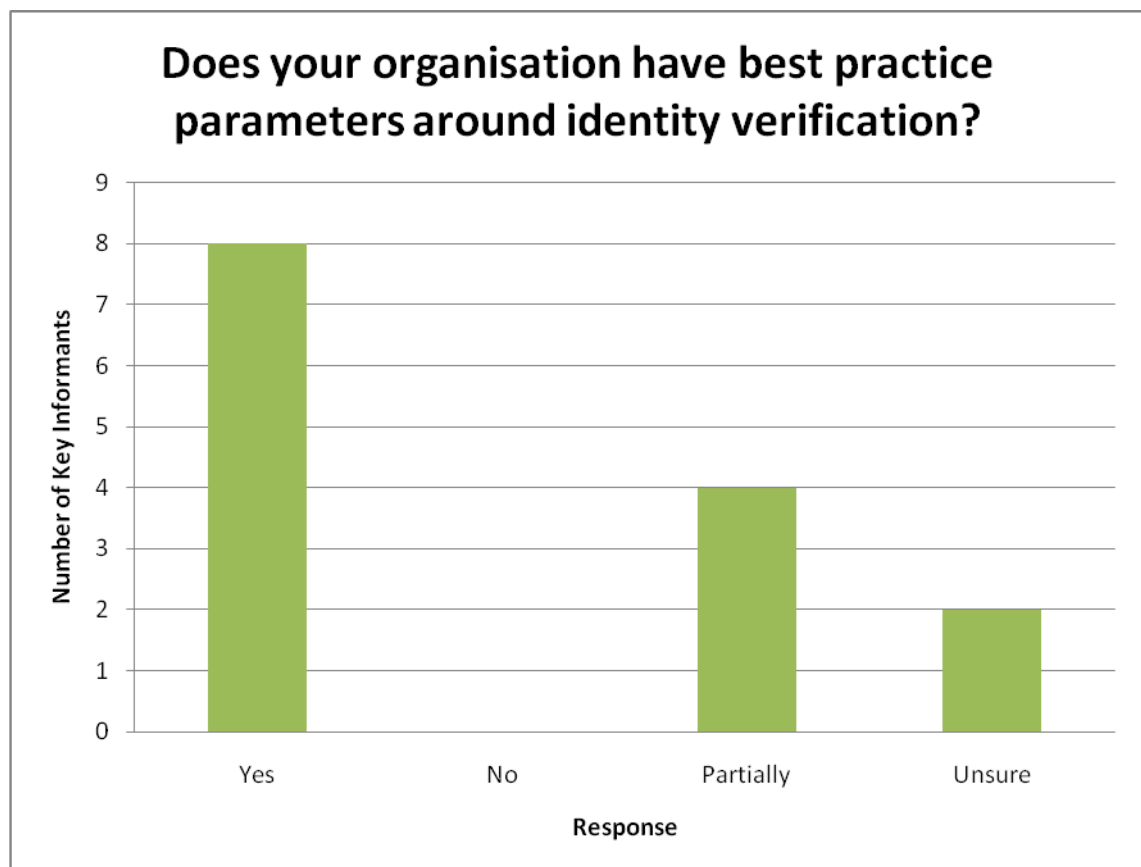


Figure 14: Does Your Organisation Have Best Practice Parameters Around Identity Verification?

‘Partially’ included those key informants who stated that their organisation had best practice parameters in one regard but not in another. This result is not surprising given that the New Zealand Government only started work in the identity fraud area relatively recently with the *Evidence of Identity Standard* being produced in 2006. This Standard has not been fully rolled out in any Government department to date. Jim Furneaux (NZTA) commented in respect of the traditionally held organisational views relating to the New Zealand driver’s licence and best practice identity verification:

Yeah we do in terms of what it is that I would expect, or one or two other people in the organisation would expect to do, if you were to turn around and say where could you find it in a document, the answer would be ‘no’ ... we’re slowly, I would say, getting the bones of best practice sorted out but not at the point where you could turn around and say here’s the document and how it will be done. And again you’ve got to bear in mind that certainly up until two years ago the simple answer was ‘the driver’s licence is not an identity document’. That was it. We’ve only managed to change that

thinking internally in the last 30 months. And now we're putting more pressure on to get a few other changes made.

There are multiple ways to verify identity and most stem from the ability of agencies and organisations to share information. This is discussed in the next section.

5.2.3 Systems to Minimise Identity Fraud

Key informants were asked what systems their organisation has that minimises identity fraud. There were 14 key informants who responded to this question and as expected, overall their answers varied depending upon the organisation in which they worked. Generic categories of responses that more than one organisation had in common were:

- Internal training of staff
- Requiring documents as part of processing
- The organisation only has basic level requirements
- Cross-checking of data with other systems
- Advanced passenger processing (APP)
- Information sharing
- Internal controls
- Identity verification
- Fingerprinting
- Lost and stolen passport database.

Training of staff at the border is imperative given that this is the entry point into New Zealand of both individuals on false identities and false documents brought in by those individuals or by mail. If either false identities or false documents are not stopped at the border, they can be used to facilitate other crime in New Zealand. Alan Thompson (NZCS) advised:

The people at the mail centre are quite clearly trained to look out for the sorts of packages and passports, student IDs, those sorts of things ... We have fraud investigators who would handle matters of falsified documentation, not necessarily passports. And training, generally, for airport people ... I wouldn't call them document experts. But the sort of thing where they'd be shown a passport. How it's been photo-subbed²². And what to look for in a photo-subbed passport ... the other thing we have loaded into our system is all of the lost and stolen passports. New Zealand passports are loaded into the Customs system.

The New Zealand passport is New Zealand's most secure identity document and has a correspondingly rigorous process associated with its issuance. Andrea Gray (DIA) stated that before a New Zealand passport is issued, the applicant's details are checked against the Online Life Event Verification system, commonly known as OLEV. This means that OLEV electronically checks to establish whether there is a birth and death record for the applicant, thus preventing individuals from stealing the identities of deceased people. In addition, each applicant's application photo is also compared against images held in the Watch List – a database of electronic images of people, stored by DIA, who are suspected of applying for a passport in another person's identity. The Watch List uses facial recognition technology to assess the compatibility of the applicant image against the database image. If found to be a match, the Watch List states the likeness of the compared images in a numerical form. Therefore, it is essential that those Government agencies that are responsible for the issuance of important documents that are often used as a form of identity, to use cross-checking of data with other systems.

Nonetheless, the issuance of the New Zealand driver's licence appears much less rigorous. When Jim Furneaux (NZTA) was asked what systems his organisation had in place to minimise identity fraud, he responded:

²² "Photo-subbed" is a term referring to photo substitution. It is used in reference to a different photo to the original being placed in a document for fraudulent purposes.

None really ... We're, I would suggest, very basic. You rock in with two pieces of paper that meet the required standard and as long as there's nothing blatantly obvious with it, then they get accepted. We don't keep copies.

The concerning issue is that staff at the AA offices that accept these documents on behalf of NZTA are unlikely to be well trained in document examination and are unlikely to be able to identify a relatively good counterfeit or forged document if one was presented. Overseas documents as well as New Zealand documents are accepted as evidence of identity for the issuance of a New Zealand driver's licence. These documents include birth certificates and overseas driver's licences. It is doubtful as to whether an AA employee would be able to identify a forged or counterfeit birth certificate from Nepal for example. Problems in this system are further compounded by the fact that no copies are made of the identity documents presented by individuals, thus, even if there is post-issuance fraud discovered, there is no documentary evidence to support the agency's case.

The *LTNZ Factsheet 20* (New Zealand Transport Agency, 2009), which refers to 'Identification for Driver Licensing' states that a New Zealand birth certificate, a New Zealand citizenship certificate or a certificate of identity issued under the *Immigration Act 1987* are all accepted as evidence of identity. However, all of these documents contain relatively unsophisticated security features and the current New Zealand birth certificate even states in bold at the bottom of the certificate: "WARNING: This certificate is not evidence of the identity of the person presenting it". Jim Furneaux was asked why these documents were accepted and his response was as follows:

If you get a driver's licence at age 15, what does a 15 year old have in terms of identity? We don't barcode them from birth ... I mean how else do you do it? I mean the 15 year old turns up and again what's been the main aim is to have a reasonable level of assurance because this is ... about identifying somebody in the system who is safe to drive. We've got to a stage now where we have to sort of wake up and smell the coffee so to speak and get

real. Now, by the same token so does every other agency ... the issues around birth certificates is, well it all requires the Registrar to issue a birth certificate. He can't issue any other form of paperwork. But if all you want it for is genealogical purposes, then why do you need a birth certificate? Or at least a birth certificate that can be stamped 'copy cannot be used' – something along those lines.

With reference to the issuance of an individual's birth certificate to any member of the public who pays for it, Jim Furneaux makes a valid point. If you are not the person named on the birth certificate, for what valid reason do you need the birth certificate (unless you are the parent of a child)? The same information can be obtained by paying for a print out of birth information which is not in the form of a certificate. Given the inherent risk in the issuing of birth certificates to members of the public, one way to mitigate the risk is to data match birth information provided to NZTA with Births, Deaths and Marriages (DIA), however when Jim Furneaux was asked whether there was any data matching agreement or similar arrangement, he replied in the negative by stating:

I mean if you think about it, it wasn't that long ago that Births, Deaths and Marriages weren't talking to each other. You know. So yeah.

Five key informants responded that their organisation had cross-checking measures in place to verify identity as part of their systems. All of these key informants were from the public sector and three of them worked for the same organisation – DIA. Mr B (DIA) advised:

Utilising our kind of unique position of having access to so much related data; to births data, passport data, citizenship data. And now we have access to AMS²³ as well ... we're not really the victims of fictitious identity by and large. If you're looking broader you can also see how we've applied technology that solves identity fraud problems. More along the lines of counterfeits and the forgeries. When people try and travel to Australia and

²³ AMS is an acronym for the computer system administered by INZ. It stands for Application Management System and holds immigration related information including the arrivals and departure for all people who have travelled in and out of New Zealand as well as travel document, visa, alerts/warnings and other immigrant information.

New Zealand we have APP²⁴ and that is a brilliant system that provides incredibly good protection and it's kind of leveraging technological advances like that, like having a good computer system, sharing information helps protect us.

Therefore, there is a great variance in the systems in which two New Zealand agencies who issue the two most common documents of identity operate. NZTA has minimal identity verification and DIA has extensive identity verification. Despite the benefits of APP as mentioned by Mr B (DIA), its role in the detection of fraudulent documents is limited insofar as the human input required in its operation. Ms F from Agency C commented:

One of the tools that we use in the New Zealand APP system, which is a system designed along the lines of the Australian APP system where people checking in from anywhere in the world to come to New Zealand are required to have the bio-data of their passport downloaded to us. It searches through our system and also through the Australian database to see if there are any alerts or visas that have been issued to those people. It then sends back a message to the airline indicating whether or not the passenger is okay to be issued a boarding pass. And in the case where it's not okay, the airline is obligated to contact us directly either by phone or by SITA²⁵ message to find out what the actual problem is and why the passenger is unable to board the aircraft. With regards to being able to identify if the document that the person is checking in with is counterfeit, or the person is an impostor, unless you've got a very very skilled airline check-in agent or you have a New Zealand ALO²⁶ there, or another ALO monitoring the flight, it's an educated guess as to whether or not there may be a problem with that document. To detect a fraudulent document, basically the tools are here on shore so we would be waiting for the person to actually arrive here. It would be difficult to know whether the document was a counterfeit one from here, if the person's checking in to come here from an overseas location. Unless of course it's from one of those economies that is attached to RMAL²⁷, which is your Australian, US and New Zealand documents, and they've been reported lost or stolen. If the document hasn't been reported lost or stolen then it's hard to know.

²⁴ APP is an acronym for Advanced Passenger Processing. It is another computer system administered by INZ.

²⁵ SITA is the name of an information technology company that administers a messaging service for airlines.

²⁶ ALO is an acronym for Airline Liaison Officer. ALOs are employed by immigration agencies in their respective countries.

²⁷ RMAL is an acronym for Regional Movement Alert List. It is a database of reported lost and stolen New Zealand, Australian and United States passports. The database is shared between these three countries.

Thus, the effectiveness of the APP system is reliant not only on the skill of airline staff to detect a fraudulent document, but also on members of the public to report their passports to NZP and DIA if they have been lost or stolen. Without the knowledge that a passport is lost or stolen, the APP system cannot prevent someone else from fraudulently using an individual's passport for travel or for other criminal means such as financial fraud. This highlights the need also for information sharing to occur between agencies so that identity fraud can be minimised. Two key informants mentioned that information sharing was a mechanism in their system.

However, the threat of identity fraud in a system could also possibly come from within an organisation. Three key informants stated that their organisations had put internal controls in place in relation to the staff that they employed. Paul Hurrell (IAG) stated that they conducted "honesty-in-employment checks" on all staff. Kate Antonievich (DIA) advised that they have integrity awareness training for all staff, police checks on all staff as well as in-built internal controls to prevent fraud from occurring, for example, it takes more than one staff member to issue a New Zealand passport. Similarly, Mr C (Agency C) said that it requires a two-person check for visa applications and this process itself is audited, however:

It doesn't make you immune to internal corruption risks. Or doesn't make you immune from missing well-executed fraud.

In terms of biometrics, two key informants mentioned the benefits of fingerprinting to minimise identity fraud. However, the NZP do not limit themselves to fingerprints.

Dave Kennedy (NZP) stated:

We have huge expertise in basic fundamental biometrics, fingerprints, not bad photographs and DNA. We also tend to interact quite intimately with people, you know, when we arrest them in particular, or deal with them, and investigate them. So often we will do active investigation of their circumstances. And we will find out a lot about those people over time. And

that's extremely valuable. Probably more so than about any other department I guess.

This comment is commensurate with an earlier statement by Kate Antonievich (DIA) in section 1.2 of the findings relating to the importance of a social footprint in society. Any interaction by the NZP with an individual, erases their anonymity under which they have been able to operate.

Overall, other systems that were employed by organisations to minimise identity fraud included:

- Early alerts and warning systems
- Discretionary acceptance of documents
- Specifying required documents for a service
- Administering a database of customers
- Cross-checking customer details with the Motor Vehicle Register
- Detection systems around payment products (banks)
- Cross checking customer details against terrorist lists
- Operating an identity management programme
- Operating a biometrics programme
- Risk targeted profiling of individuals travelling to New Zealand
- Active investigations of individuals
- Referring individuals to a specialist unit for investigation
- Bio-data checking
- Ongoing research into identity fraud
- Operating on a Virtual Private Network

This section has reported the current systems issues and the next section examines the improvements in the current systems that key informants would like implemented.

5.2.4 Improvements in Systems to Combat Identity Crimes

Key informants were asked what improvements they would like to see in their organisation's system to combat identity crimes. From the 15 key informants, one key informant deleted their answer to this question and three key informants were not directly asked this question. A summary of the improvements sought by the remaining 11 key informants is represented in Figure 15.

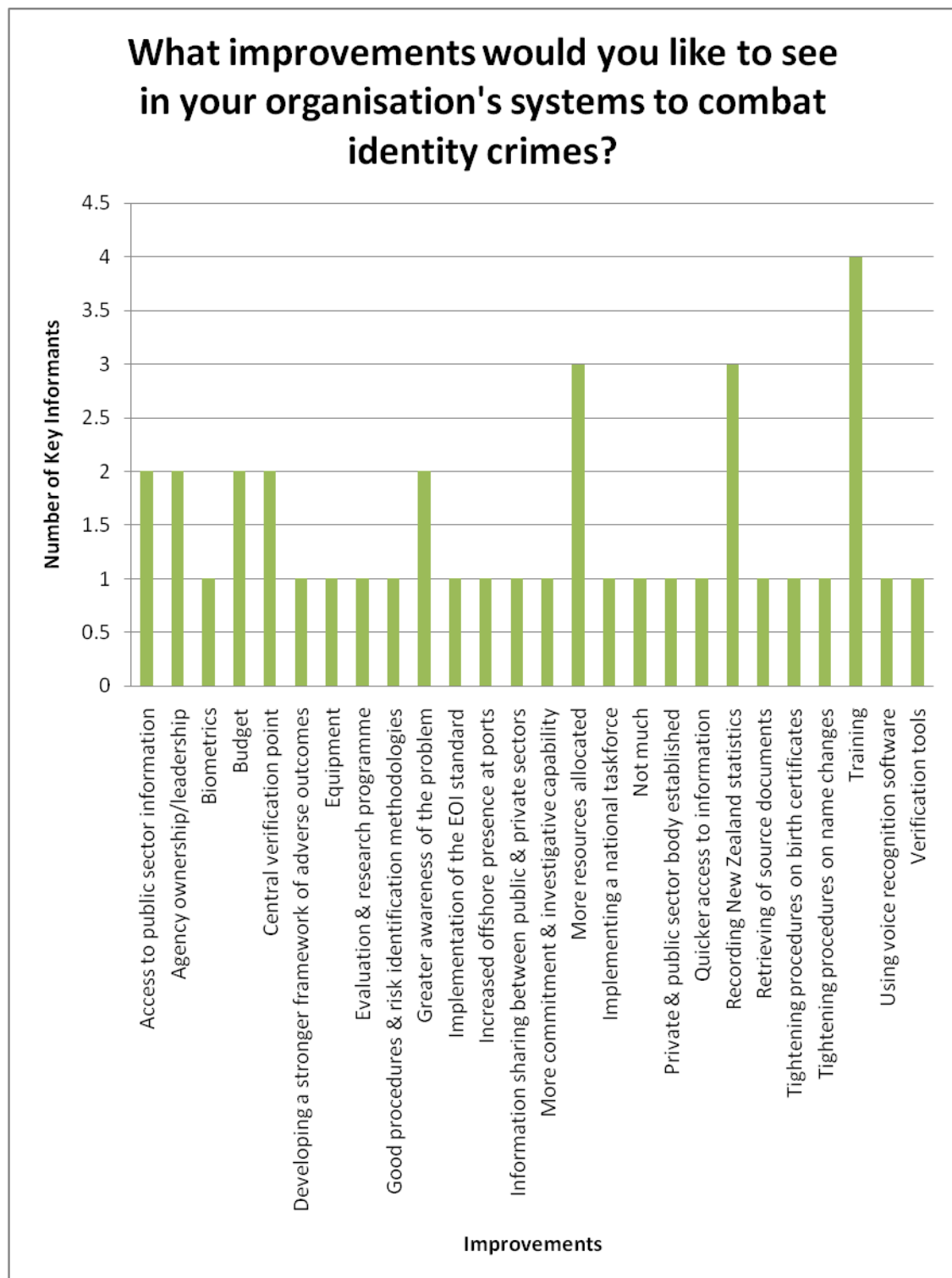


Figure 15: What Improvements Would You Like to See in Your Organisation's Systems to Combat Identity Crimes?

The most mentioned improvement needed in an organisation's system was 'Training' with four key informants (all from the public sector) citing this area. Mr C (Agency C) stated:

Do we have robust enough guidelines for staff about when to do identity verification; so they have the training and skills to know how to go and do it when they need to do it? How do we record what we've done? How do we record when we find it? And then supporting IT systems.

Despite four key informants specifically stating that more training was needed, two key informants stating that a bigger budget was needed and one key informant stating that more equipment was needed, three key informants stated generically that an increase in resources was needed in their organisations. Dave Kennedy (NZP) commented:

I'd like to see my unit be given more resource, I'd like to see the whole area given more resource and more commitment.

However, budgetary constraints were summed up by Mr H (NZP) who stated:

It's like most things here – they're bound by a limited number of taxpayers and a small budget and the need. How much damage does identity crime actually cause in terms of fiscal losses?

Similar sentiments were expressed in the private sector with Mr A (Bank A) advising:

Let's start recording the statistics so the Government ... New Zealand gets a handle on just how much identity fraud is ... the Australians record it. It's an actual crime on their books. They have statistics they can produce on how many cases there are in a year. How much it's costing. Until this country and I guess the taxpayers realise how much it is costing us then nothing's really going to happen.

The lack of statistics was an issue identified in section 1.2 of the findings. It is more deeply discussed in the next section in the context of its place in the identity fraud system.

5.2.5 Identity Fraud Cost and Statistics

Each key informant was asked whether their organisation collected identity crime statistics. From the 14 key informants who responded to this question, 11 stated that their organisations did collect statistics while three stated that their organisations did not collect statistics. Notably, these three were all from the private sector.

However, the key informants' responses were not all black and white. Some organisations did collect statistics, however, they were not specifically categorised as being a result of identity crime. This was particularly in the case of the financial sector organisations where, for example, if a fraudulent identity was used to perpetuate credit card fraud, that organisation would label that statistic as credit card fraud rather than identity fraud. In addition, the reporting of identity crimes in the private sector could be seen as exposing vulnerability in their systems to the public and their competition, thus degrading their reputation or integrity. Justin Kerr (FSF) noted:

Partly there would be a bit of concern about publicity surrounding these areas of vulnerability ... I mean there are plenty of isolated cases that hit the press and you do see prosecutions reported every now and again but there would be an awful lot more happening that isn't evident from the newspapers.

In the public sector, agencies commonly report incidences of identity crimes to a database which is held and operated by the New Zealand Police. This possibly explains why all key informants from the public sector advised that their agencies did collect statistics. Nonetheless, the Police database relies on ad hoc referrals from other agencies and it is doubtful that all agencies and all statistics are reliably captured in this regard. Dave Kennedy (NZP) added:

It's reliable and valid in as much as what it is but it doesn't represent the true volume that could be reported. It's vastly under-reported at this time. And the reason is because it's very difficult to distinguish from other offences and we have to implement entirely new ways to measure it. Identity crime is after all an artificial classification.

In New Zealand, there is no *direct* offence or legislation in relation to identity crime or fraud, hence the reference to it being an artificial classification. This could also be the explanation as to why, despite the fact that statistics are kept by public sector agencies, that no key informant really knew what identity fraud was costing their organisation (see Figure 16).



Figure 16: How Much Has Identity Fraud Cost Your Organisation to Date?

Of the 14 key informants that responded to this question, 12 stated that they did not know how much identity fraud had cost their organisation to date. The one key informant who replied 'Nothing' was Ron Watt (BNZ) whose answer related back to the issue of the way in which statistics were classified:

I have to say nothing, because we don't classify it as identity fraud ... the potential there is large depending on what is classified as identity theft ... People stealing other people's credit cards, if you were to classify that as identity theft because they have stolen something that belongs to someone else that could probably run into, as an industry, millions of dollars.

The key informant who stated that identity fraud had cost their organisation 'Lots' was Ms F (Agency C). When asked if there was a specific figure, she stated that as a guideline, if someone was allowed to travel to New Zealand under a false identity then that would cost the New Zealand \$50,000 per annum. Ms F advised that this cost was ongoing:

And then ongoing from that is the social costs. The person may be of ill health which impacts on our medical services. The person needs to obviously live somewhere so they have to be accommodated so that impacts on the Government's housing system. They'll obviously have family or children that, you know may have travelled with them so there's education it impacts on as well. If these people have been in criminal activities in other places then that also impacts on the security side of things. They become a problem to the Police. They become a problem to the New Zealand public. It has a huge impact on New Zealand if we don't get it right.

Moreover, Mr A (Bank A) expressed his frustration at the lack of both statistics and a figure on identity fraud:

We're like the Police, we don't keep a specific tally of identity fraud or results and most of our fraud out here is probably related to identity fraud in one way shape or form. I steal your cheque and pretend I'm you know you to cash it or whatever. So yeah, you could say it's identity fraud but no there's no hard and fast stats between any of the banks ... We're cracking on that. We've been pushing the Police and everything. Well I know the Police have an identity crime unit but I think there's only about two people in it. And this is a huge issue – this goes right across all industries. It's certainly been something that Government's been lacking in, lagging.

Other countries such as Australia and the United States of America, have managed to estimate the cost of identity fraud to their respective economies, however, the reliability of these statistics is questionable. Issues such as *how* these statistics are being calculated is relevant, given the reluctance of organisations to report identity fraud. Nonetheless, these countries have moved forward legislation-wise with specific legislation being adopted in relation to identity fraud offending. This may explain their ability to measure it as an offence and cost to the economy. New Zealand has yet to move in the same direction.

5.3 FRAMEWORKS AND LEGISLATION

5.3.1 Frameworks

The New Zealand Government has been developing work in the identity arena with the overarching strategy named the Identity Assurance Strategy (IAS) (New Zealand Ministry of Justice, 2009). Kate Antonievich (DIA) explained:

An Identity Assurance Strategy for Government which is much broader than DIA but we led the work to put it together. And one of the key drivers for that was to better protect Government from identity fraud. It's a strategy that's got a whole lot of initiatives that Government agencies were meant to implement including us.

The *Evidence of Identity Standard* (EOI) (New Zealand Department of Internal Affairs, 2006) is an identity framework that is an element of the larger Identity Assurance Strategy. Ms G (DIA) explains how the EOI Standard fits within the Strategy:

The IAS ... as its name implies is about increasing particularly Government agencies assurance about the identities that they're dealing with and how they actually deal with identity itself. As part of that there's the EOI Standard which provides the framework for agencies working with establishing identity, what the core components are that they should be looking at, and the assurance levels that they need that the identity that they're verifying and establishing, is the identity itself. The nature of the transaction or the nature of the product affects what level of assurance within the EOI framework that they need to be working to. So the IAS is broader, of which EOI is one element.

Key informants were asked whether they were aware of the *Evidence of Identity Standard* (EOI) produced by the DIA in 2006. From the 14 responses received for this question, nine key informants said that they were aware of it; however, three of these key informants were from the DIA (the custodian of the Standard). Five key informants advised that they were not aware of the EOI Standard. One of these key informants was from the private sector. Key informants were subsequently asked whether the EOI Standard had been implemented into business practices in their organisation. From the nine key informants who stated that they were aware of the EOI Standard, one key

informant said that the Standard had been implemented, three key informants stated that it had not been implemented and five key informants stated that it had been partially implemented (three of five key informants were from the DIA).

The one key informant who stated that the EOI Standard had been implemented into his organisation was Ron Watt (BNZ). However, his statement was qualified as follows:

I really think that it has always been there. It's not something which is brand new to us ... It is just part of our culture to be that way.

This response indicates that the BNZ has had its own policies for dealing with identity standards as part of their systems. The EOI Standard has had only partial application in some public sector agencies. While it has been written as a generic standard, it appears that its complete applicability in all systems is in doubt. When asked if the EOI Standard had been implemented in his organisation, Mr C (Agency C) commented:

That's part of the OAG²⁸ project – we have done an assessment two years ago. And we believed we were broadly compliant. But we are doing much more now, because the EOI Standard's evolved, there's now better guidelines and check lists. We're redoing our risk assessment right now with DIA – and redo the application of the EOI Standard in our systems. We have a view that we actually need to develop an amendment to the EOI Standard to reflect the types of issues with overseas identity establishment.

Those key informants, who advised that they were aware of the EOI Standard, were asked for their views on the Standard. Justin Kerr (FSF) cast doubts on the effectiveness of the EOI Standard in its applicability to the private sector. He stated:

It's extensive. It's amazing only large organisations who can put a terrific lot of effort into business process could contemplate taking all of those steps themselves ... it's very much a Government thing ... if you'd done absolutely everything that they're suggesting that you might do, you would run out of money and your business would've gone bust ... I don't know that it's realistic to do that. That's why it becomes so important that there be a lower cost, particularly if ... part of the identity requirement that financial institutions have to meet is beyond their business need. It's to meet other international

²⁸ OAG is an acronym for Office of the Auditor-General.

legislative requirements. And when you get into that space, you do need the Government to ... provide a little bit of help ... I mean it really is just off the deep end ... We can't necessarily ... live our lives in that way.

Nonetheless, Jim Furneaux (NZTA) commented that the EOI Standard has been improving and that further cross-agency work should continue. However, the cost factor does not escape public sector agencies. He noted that cost was going to be a major factor in deciding whether or not the Standard would be implemented:

So you can bring in a Standard and there's all sorts of things you can do like turn round and ascribe points to certain pieces of documentation. So if you do that you're adding one level of security ... a feel-good sort of security factor. But there is a cost with that ... the issue is actually about balancing all that. Will every agency subscribe to it? Will they be made to subscribe to it? Are they going to water it down and say well okay, this is something we recommend that you do? Will they say, well okay Minister for us this is going to cost ... so many transactions, at so many minutes or seconds per transaction? Where are we going to get that money from? The driver's licence fee is 'x'. Well we don't want people to pay that much money. Are you going to give us that money? 'No, we're not'. So what happens? The Standard doesn't get picked up. That's where the problem is going to be. Not so much in the Standard itself ... There's got to be a commitment to it.

Despite the challenges that both the private and public sectors possibly face in implementing the EOI Standard in the future, its development per se has benefits according to Dave Kennedy (NZP), due to the absence of any other work done in the identity processes field in New Zealand:

I think that the EOI Standard is great in that it's the first time anybody's actually done anything like it and so it's extremely valuable in that regard. I don't think it's particularly accessible. But I promote it every chance I get. I promote it in the private sector because at least it gives people a blueprint ... the private sector might say 'we can't afford to do this Standard' – well, it's like tough, maybe you should ... it's equally difficult for Government to do it. Where it's really useful though is just to even get people thinking about a process ... when you look at identity processes in New Zealand, very little thought has been put into most of them. Outside of DIA and arguably inside DIA, most identity processes are just ad hoc and slapped together.

The EOI Standard is an extensive document, being 128 pages long²⁹. The effects of its content will impact upon organisational systems in multiple ways and by no means, is the Standard a document that can be implemented overnight. It is essentially a blueprint for an identity verification system. The DIA has not even implemented its contents into all of its systems to date, given the complexity of its implications. Kate Antonievich (DIA) explained:

The problem with things like Passports and Citizenship is that any fundamental change to the overall process, particularly if you want to do it in an online manner, literally takes years while you ... rebuild your systems as well as your ... internal processes and so on ... Births, Deaths and Marriages is different because of the nature of the open registers and for example, the new legislation.

Andrea Gray (DIA) added that the EOI Standard was being evaluated by being piloted in three different agencies: Citizenship (DIA), IRD and LTNZ, commenting:

Part of the evaluation of that pilot will be to determine what the difference would be if the Standard were implemented.

Moreover, the EOI Standard is just part of a programme of work around identity. Kate Antonievich (DIA) advised that work has been publicly funded for the:

Data Validation Service (DVS): An online system which enables agencies to check whether identity information legitimately exists. Its limitation is the fact that the agency will still need to ascertain whether the person holding the document is the legitimate holder.

Identity Verification Service (IVS): A system where individuals register with the IVS and their identity is comprehensively authenticated. Their details are subsequently logged with the IVS and an individual is able to log on and authorise agencies to view their identity credentials.

²⁹ In 2008, an amendment to the EOI Standard was published. It is four pages in length.

In addition, Andrea Gray (DIA) stated that her organisation is part of the Border Sector Governance Group. This Group is made up of Chief Executives from the following public sector agencies: DIA, DOL, NZCS, MAF, MOT, NZFSA and produced the *Border Sector Strategy 2008-2013* (Border Sector Governance Group, 2008). The Group's aim is to improve the effectiveness and efficiency of New Zealand border processes. In terms of DIA's role, Andrea Gray advised:

The role we're going to be playing is to develop the advisory and informational structure around the use of biometrics at the border and the standards for these biometrics ... working with the border sector as a whole to understand the risks, the identity-related risks that occur at different parts of the border process there ... the large border system. So we're leading the identity-related work in connection with the border.

Despite the progress being made by inter-agency programmes with respect to identity fraud, there appears to be no foreseeable change in New Zealand's legislation that supports any specific focus on identity fraud. Legislative issues are discussed in the next section.

5.3.2 Legislation

Key informants were asked what they thought of the current legislative provisions for identity fraud offences in New Zealand. Responses were received from 14 key informants and these are outlined in Figure 17.



NOTE: IVS is an acronym for Identity Verification Service; BDM is an acronym for Births, Deaths and Marriages.

Figure 17: What Do You Think About the Current Legislative Provisions for Identity Fraud Offences?

Four key informants stated that identity fraud offences are currently covered by the Crimes Act 1961, however, only two key informants advised that the legislative provisions for identity fraud related offences were adequate. One key informant commented that legislation catered for Passports, Citizenship and Births, Deaths and Marriages and that new legislation was being developed for the IVS. Only one key

informant, Dave Kennedy (NZP), believed that there are robust laws in New Zealand but noted the absence of any identity crime offences:

Well at present and I don't believe there is a need, we have an absence of any offences around identity crimes. The only thing that's been proposed to me from offshore police is possibly the possession of identity documentation and information as an offence. In the same way as having possession of utensils for drug use is an offence ... but I think that when you look at our computer crimes, our general theft provisions, and our fraud provisions in New Zealand as well as the plethora of other offences, the only area that really could do with sharpening is the Tax Act. Because they don't seem to think that it's an offence, or have an offence, for misusing IRD numbers and obtaining IRD numbers in fictional names. Or if they have, it's so insignificant that it's not worth their attention. But overall ... we've got very robust laws and they're actually quite easily applied to virtually every situation. I have not yet encountered an identity crime situation that hasn't had an offence covering it. And we've been looking.

Nonetheless, overall opinion from key informants was negative in relation to this question with one key informant going as far as saying that current legislative provisions perpetrated fraud. Jim Furneaux (NZTA) advised:

In terms of driver licensing they are woefully inadequate. They actually assist the perpetration of fraud – because we simply cannot use the legislation to investigate and prosecute.

Two key informants also believed that current legislative provisions for identity fraud did not cover the true nature and extent of identity fraud in New Zealand. Paul Hurrell (IAG) responded:

Once again I don't think it's kept pace with what's actually happening out there ... we've just had a revamp of the Crimes Act and had a sort of a catch-all provisions in relation to computers and all that sort of thing come in. But it doesn't address identity fraud as such. I think there must be provisions under ... Births, Deaths and Marriages Act in relation to using identities and that but I'm sure the penalties are probably ridiculous. Haven't seen them but I can imagine what they're like. Fifty dollars or something like that.

A total of three key informants stated that penalties in legislation were weak, with one key informant commenting that the legislation was tough but the sentencing was weak. Mr C (Agency C) advised:

I think the legislation is pretty tough, it just seems to be the sentencing. I think the judiciary is slowly coming around to a recognition of what impacts identity crime has. I think in the past it might have been seen as a victimless crime or harmless almost. But I think some of the scale of some of the identity crime has increased. And whereas a crime in the past might have been seen as a say benefit fraud, I think that there's a recognition now that behind that there is a more serious crime. Obviously the increased sensitivity to national security, terrorist type things has also placed a greater realisation that now identity crime is a serious problem. But I've seen people who get wet bus tickets slapped on the wrist for fraudulent passport prosecutions that Police have taken out of some of our recent investigations. I have noticed the sentencing seems to be getting tougher over the last few years.

Ms F (Agency C) explained the repercussions of weak legislative penalties:

Although we have the power to put them into a term of imprisonment and charge them \$NZ20,000 ... the actual maximum has never been utilised ... the judges should be sending these people away for huge amounts of time, rather than small amounts of time like six months. Or because they've already been in jail for three months already, they've already done three months, so the judge decrees that that's long enough in prison, and now they can be shipped out. Once we ship them back to their home country, it doesn't take them long to connect on to a new identity and start all over again. Because when they arrive back in their home country there's no police to meet them, they're not taken back into a prison situation when they get home. They're just allowed to roam free again. And they'll be back. They'll just come back under another identity and we'd never know.

Two key informants from the banks said that there were no legislative provisions for identity fraud offences in New Zealand:

There isn't any really – that's the problem ... There's nothing under the Summary Proceedings Act that I'm aware of that is specific to taking over an identity or misleading ... misrepresenting who you are. Australia do. That is a specific offence over there. Mr A (Bank A).

What legislative provisions? When you look at what they're trying to introduce in Australia, when you look at the UK ... it makes me repeat the question – what legislative provisions? Ron Watt (BNZ).

Key informants were also asked whether they thought that current legislative provisions acted as a deterrent for identity crimes. From the 14 key informants who responded to this question the results were as follows:

- 9 key informants thought 'No'.

- 3 key informants thought 'Partially'.
- 1 key informant thought 'Yes'.
- 1 key informant was unsure.

All 4 key informants from the private sector expressed concern relating to the lack of deterrents in current legislation relating to identity crimes. Mr A (Bank A) stated:

They're non-existent in ... white collar type crime – you can get caught – it's just a smack on the hand with a wet bus ticket. But if you bash someone up at the ATM you might get a couple of years. You put somebody through hell ... by taking a \$300,000 mortgage on the house and then letting go into arrears 'cos you've scarpered with the money ... All the despair and grief.

Paul Hurrell (IAG) commented:

Even the penalties aren't there. They've got to be stronger penalties. And even if the penalties are there, by the time you get through the Court process, everything's just watered down again ... in Australia you have fines and if you breach it, if you're fined \$200,000, you pay \$200,000. That's more a deterrent to anybody than anything else.

The reasons why New Zealand legislation does not provide a deterrent for identity fraud offending varied between key informants in the public sector:

We simply don't prosecute people because it's too hard. At the end of the day it's generally come to us in terms of a fiscal fraud somewhere, Police may follow up, and it may get a mention in the Summary of Facts³⁰ that a driver's licence was involved ... It's just simply an offence of fraud and they use the document, namely a driver's licence, to commit that fraud. That's most often the way it's put. Whereas simply getting a prosecuting agency ... to turn around and say AND an offence was committed against the driver licensing and it's another line on the Caption Sheet³¹, which has another penalty attached to it, would be a start. Jim Furneaux (NZTA)

It's not seen as being a serious crime, if you like, as theft. I think a lot of people are skirting around the margins of identity crime don't see it as actually illegal ... I think there's a naivety about being offended against, and I think that there's a naivety around offending here. Mr H (NZP)

³⁰ A Summary of Facts is a summary of the circumstances against an offender that forms the basis for the offender being charged.

³¹ A Caption Sheet is a summary of the charges that an offender has been charged with under legislation.

If you look at the sort of people who use identity crime as a way of trying to get into the West from desperate situations, those incentives are strong ... and when they get here, if they're successful, the benefits are huge ... financially, lifestyle, access to health and education ... I just think people in New Zealand are naive about the motivational incentives that drive illegal migration. At the other end, the sort of more evil identity crime that's done by organised crime for trafficking. Mr C (Agency C)

The lack of enforcement and the penalties that are actually applied, can't possibly be a deterrent. Dave Kennedy (NZP)

One of the key informants who believed that New Zealand legislation partially acted as a deterrent for identity fraud was Mr B (DIA) who stated:

Perhaps certain pieces of legislation may act as a limited deterrent ... criminals tend to, it appears, fear more the risk of capture, apprehension, than they do what's going to happen to them, because they have no control over what's going to happen to them. Be it a slap over the hand with a wet bus ticket or be it a \$250,000 fine – they have no control over that. What they're more concerned about is 'am I going to get caught?'. I don't want any type of punishment. Which do you want, one poke in the eye or three? It's like I don't want any of them ... So you need to get ... the systems in place to ensure these people are going to be captured, apprehended, detected than necessarily purely just punishment alone ... And if a criminal sees both ... the whole picture that they face a great risk of getting caught and if they do get caught it's going to be something nasty as well.

The one key informant, Mr D (Agency D), who believed that current legislative provisions provided a deterrent to identity fraud, qualified his answer as follows:

The recent amendment to the Crimes Act that incorporates electronic fraud for example, they always need to be reviewed because there's always someone willing to try and beat the system. So the current legislation is adequate I'm sure ... if there's a person offending in New Zealand online it can be really difficult, or where they're in another country, it can be really difficult to obtain the information ... because some countries have different legislations, and it could be that I just can't ring up someone in New Zealand who's a provider and say please give me the details of an account holder ... it's really frustrating that sometimes the legislation isn't geared in a way to make things easy for the investigator.

In summary, the *Identity Assurance Strategy* is the overarching identity related programme which encompasses the EOI Standard. This Standard is a framework for organisations in which to implement comprehensive identity procedures. Nonetheless,

this work is largely in its infancy, only having been piloted in three organisations to date. Issues raised by key informants mainly revolved around the cost of implementing such a comprehensive regime into current business practices. Moreover, there is no provision for *specific* identity fraud related offences in current legislation. Identity fraud is generically covered by the *Crimes Act 1961*, however it has limited ability to act as a deterrent with both lack of enforcement and weak penalties being negative factors. New Zealand appears, in this regard, to be lagging behind other countries such as Australia.

6 CONCLUSION

Identity fraud has been described as the fastest growing crime in the world and New Zealand has not been immune from its destructive capabilities. The onslaught of the online world has created opportunities to conduct business in a faster manner; however, it has opened the doors for criminals to more anonymously commit crimes. Society in general has moved away from face-to-face contact with an increasing number of transactions taking place online from behind a computer. Moreover, the public availability of software has given individuals access to some of the technology necessary to reproduce identity documents. Over time, professional counterfeiters eventually succeed in reproducing security features in some of the most secure identity documents such as a passport. Failing this, false identity packages containing identity documents are readily available for purchase on the Internet. Counterfeit and genuine New Zealand passports have been found in law enforcement operations overseas, targeting counterfeiting and people smuggling rings. Thus, New Zealand is often reliant on foreign agencies to pursue any prosecution action as the offence occurred outside of New Zealand. New Zealand's borders have also been regular targets for illegal immigrants who have travelled here on false, forged or counterfeit passports, often under fictitious or stolen identities.

The three main reasons that identity fraud is committed are for financial advantage, illegal migration or for the concealment of another crime. Identity fraudsters range from individuals to organised crime groups and terrorists. Nonetheless, the blasé public attitude and naivety towards identity fraud in New Zealand encourages identity fraudsters to operate in this country. In addition, there are systems weaknesses in New Zealand that enable identity fraud to occur. Organisations in New Zealand employed a

number of methods in an effort to curb identity fraud. These varied and included such measures as the use of biometrics, early alerts and warning systems, risk targeting and active investigations. Desired systems improvements were also varied with the most desirable being staff training, however, an increase in overall resource allocation was also a requirement. No organisation knew exactly how much identity fraud was costing them financially.

The main human threat of identity fraud in New Zealand comes from organised crime groups, whether they are internationally or domestically based. A major concern regarding identity fraud is that it is a breeder crime for other crimes. An increase in mortgage fraud and credit card fraud were stated as issues in the private sector. A breeder identity document could be a birth certificate or a name change certificate and there is further concern as to how easy it is to obtain another person's birth certificate and how easy it is to change one's name in New Zealand. Such documents can be utilised in obtaining a New Zealand driver's licence, which, in the absence of a national identity card in New Zealand, has become a de facto identity document. Prior to 25 January 2009 when the *BDMRR Act* came into effect, even foreign nationals were permitted to change their name in New Zealand (now an individual must be a New Zealand permanent resident or citizen). However, there is no verification pre or post name change to check the veracity of the information provided. It is therefore a systems weakness, that the births, deaths, marriages and name change information is not readily available for law enforcement purposes to all other public sector agencies. While one can consider that these documents should not be utilised as identity documents, the reality is, that they are accepted and have a history of being used to perpetuate identity fraud. It was reported that birth certificates were the most widely abused document in New Zealand, followed by driver's licences and passports.

However, identity verification in New Zealand is not easy, especially for the private sector, which faces reputational and financial damage from any cases of identity fraud, but cannot be provided private information from public sector agencies due to restrictions under the *Privacy Act 1993*. The verification of overseas identity documents is even more difficult and the security standards of overseas documents may not be of the same standard as New Zealand documents. Furthermore, concerns relating to current identity verification procedures included a lack of staff training and a lack of biometrics used in New Zealand systems.

The term *identity fraud* itself has been examined very little in academic literature but is used abundantly in everyday life. International data on identity fraud faces issues around reliability and validity. This is due to the fact that there are no international standards for identity fraud offences, classifications and general terminology. In addition, one identity fraud offence may stretch across more than one jurisdiction and more than one agency and therefore, be counted more than once in the data. There are no official public sector statistics in New Zealand on identity fraud and no official systems in place to measure incidences of identity fraud. However the New Zealand Police administer a database of false or misused identities. The success of this database relies upon public sector agencies informing the Police of cases of identity fraud.

Despite identity fraud being the fastest growing crime, the fact that it is easy to commit identity fraud in New Zealand, the fact that it can be committed with speed, the fact that it is an enabler of other crimes, the fact that the New Zealand *Organised Crime Strategy 2008-2009* stated it is an “integral part of organised criminal offending”(New Zealand Ministry of Justice, 2009, p. 4), the fact that the United

Nations Intergovernmental Expert Group advised “systematic and structured processes for gathering and analysing data” (OECD, 2009, p. 100) be created, the fact that New Zealand’s biggest benefit fraudster used 123 identities, the fact that New Zealanders are concerned about the misuse of their identity, the fact that the Office of the Auditor-General conducted a review into identity fraud at INZ and that it is at the very core of any system, only one government department (DIA) has an *outcome* around identity and there is no *specific* identity fraud legislation in New Zealand.

Minimising the risk of identity fraud relies on robust systems in which the ability to verify identity is paramount. There are flaws in our own systems in New Zealand which assist in the facilitation of identity fraud. Examples include:

- The State Services Commission promotes a whole-of-government approach to solve issues; however, information sharing is often negated by various interpretations of the *Privacy Act 1993*. In addition, activities which take priority in various agencies differ as resources are limited.
- The ability of the New Zealand Government to work with the private sector in New Zealand is largely hindered by the *Privacy Act 1993*. This works in the favour of identity fraud criminals as identities are unable to be comprehensively verified against official records.
- The ability to change one’s name in New Zealand is easy, yet even government departments must apply for and pay to get this information from DIA – which affects the heart of the identity system. A barrier to obtaining this information efficiently has been imposed by legislation which states a fee must be paid for the information. It is ironic that DIA is leading identity-related work in New Zealand, yet one of its own business units is facilitating identity fraud. The ease

with which one can change one's name enables a large amount of identity fraud to occur for financial gain. Even with the establishment of the new IVS, if an individual does not have a passport (which would link his/her identity data), with every name change that have, they can create another identity with the IVS. Therefore, there is potential for one person to have multiple identities on IVS and this leads to possibility that agencies will be fooled into a false sense of security that who they are dealing with online, is in fact that person. Moreover, there is no way of preventing individuals from giving their password and logon details to another individual for use online.

- The New Zealand driver's licence has become a de facto identity document in New Zealand, yet insecure documents are accepted as evidence of identity and verification is rare, especially in the case of overseas documentation.
- IRD secrecy provisions in legislation prevent it from sharing information with other government agencies.
- Data entry of identity information into electronic systems is not always accurate.
- New Zealand defers to poorer South Pacific countries that are in the realm of New Zealand (Tokelau, Cook Islands and Niue), that often lack the same integrity standards as New Zealand. Actions of these countries impact upon citizenship by birth entitlements in terms of the *Citizenship Act 1977*.
- IRD and NZTA issue IRD numbers and New Zealand driver's licences respectively to people without verification and who are often overstayers.
- An individual can establish a company in New Zealand without having to provide any identification.

- The verification of overseas identity documents is difficult for public sector agencies in New Zealand, but more so for private sector organisations.

New Zealand faces international repercussions from failing to address identity fraud. The integrity of the New Zealand passport is at risk, as is our visa free status with over 50 other countries. New Zealand is also a signatory to United Nations conventions and agreements, such as in relation to human trafficking and people smuggling. Exposing New Zealand's weaknesses could potentially mean international reputational damage and punitive action by the United Nations or the greater international community. Nonetheless, public policy solutions to identity fraud are fraught with international and domestic political and social issues. Identity policies are also complex and costly. The issues that the New Zealand Government is faced with in developing public policy on identity fraud are as follows:

- The reliability and validity of organisational data;
- The cost and reliability of new technology as well as the synchronicity of the technology across agencies and older systems;
- How to adhere to the *Privacy Act 1993*, while still sharing information between domestic and international agencies;
- The development of legislation that will be a suitable deterrent to potential identity fraudsters;
- The allocation of Government resources and measuring the feasibility, effectiveness and efficiency of these resources.

The following issues require further research by the New Zealand Government before any policy or legislation is firmly set in place:

- How to overcome jurisdictional issues when offences occur outside of New Zealand (but may have affected New Zealand);
- How to develop outcomes that are meaningful and transferable across public sector agencies. Corresponding outputs must be created that truly reflect an outcome to minimise identity fraud;
- Domestic and international politics. At home these may include accusations against the New Zealand Government of 'big brother' behaviour while internationally, the collection of biometric information could become a standard;
- Education of the public to effectively minimise the risk of identity fraud to themselves;
- The development of reactive versus proactive policies to instances of identity fraud. Consideration must be given to where funding is necessary;
- The concept of risk versus facilitation. Policy which hinders law-abiding citizens from obtaining goods or services in a timely and cost-effective manner, as a consequence of increased security measures is not desirable. A balance needs to be sought;
- Identifying what the catalysts are for change in identity management. Investigation is necessary into the weaknesses in the system and threats against the system so that the appropriate changes in policy can be effected;
- Custodial issues in respect of who 'owns' the policy and who is going to be accountable for the policy outcomes;
- Overall, the mechanics of how a policy and legislation works at an operational level is essential if the risk of identity fraud is to be minimised. The development of working groups with key frontline staff is recommended.

While DIA is developing the Identity Verification Service, the Data Validation Service, the Identity Assurance Strategy and has developed the EOI Standard, the private sector in New Zealand needs help. Any case of identity fraud costs financial institutions money and these are costs that will ultimately be passed on to other customers for the resources to contain identity fraud. It is envisaged that the EOI Standard may be utilised in the private sector but the financial industry stated that it was too costly and cumbersome to be of any use. Moreover, while the strategic frameworks around identity assurance are slowly coming together and pilot programmes are beginning in a select few agencies for the EOI Standard, identity fraud is continuing to occur with speed throughout the country. At a tactical level, the New Zealand Government needs to quickly implement some practical capabilities to stem the incidences of identity fraud from occurring.

In order for New Zealand to capture the identity fraud environment in New Zealand and ultimately contain the occurrence of identity fraud, the Government needs to formally and centrally develop an identity policy. An identity policy would provide a core from which outcomes around identity fraud can be established throughout public sector agencies in New Zealand (see Figure 18 on the next page). The identity policy would clearly state the objectives of the policy and what it aims to achieve. Once the outcomes are identified and the associated outputs are in place, specific legislation can be developed and implemented. This legislation would benefit both identity fraud prevention and identity fraud enforcement by defining identity fraud offending. A focus on identity fraud from an identity policy at the top would enable identity fraud statistics to be analysed and collected from enforcement records and the subsequent

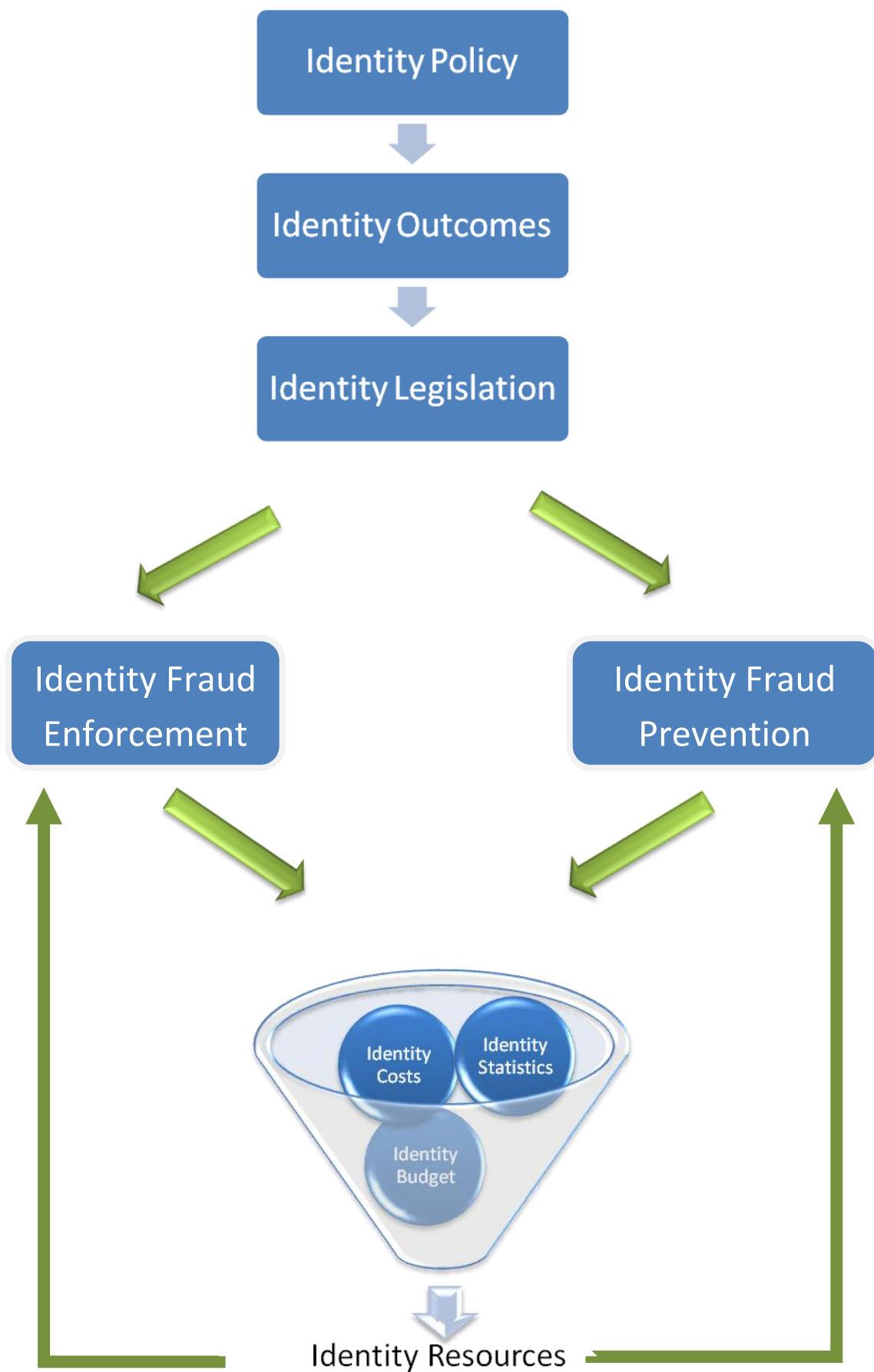


Figure 18: Capturing the Identity Fraud Environment in New Zealand - An Identity Policy Led Model

costs to the economy calculated. This would enable the Government to accurately budget for identity fraud costs which would pinpoint the amount of money to put into resources to reduce identity fraud. These resources would subsequently be fed back into the identity fraud enforcement and prevention programmes, where their strengths and weaknesses can be assessed against identity outcomes, legislation and ultimately contribute toward further statistics, cost and budgets toward fighting identity fraud.

The New Zealand Government has an advantage over many other countries in the fight against identity fraud in that official records held on people who live in New Zealand are largely centralised. This should assist in facilitating open communication and information sharing between domestic agencies, as there is no state level government with which to contend. However, in New Zealand various public sector agencies' systems conflict with one another in that one agency is attempting to combat identity fraud and another is enabling it to occur. Of further concern is that identity fraud can occur with speed and the detection of an identity fraud offence may not be uncovered until years after the offence has occurred. Not all identity fraud offending is prosecuted due to the time passed since the offence, jurisdiction issues, cost, agency priority or political issues.

New Zealand legislation contains elements of identity fraud offences but the offending is often classified as something else, for example, immigration fraud, credit card fraud or benefit fraud. The non-classification of identity fraud as an offence in New Zealand per se has led to a lack of statistics and therefore, a true understanding of the identity fraud environment in New Zealand. New Zealand is behind other similarly democratic western countries – Australia, Canada, United Kingdom and United States who either have or are in the process of introducing legislation specifically relating to identity fraud. Both private and public sector agencies in New Zealand have reported that

current legislative penalties in New Zealand for identity fraud offences are not effective and are inadequate (with the exception of the Police). It was further reported that the benefits of committing identity fraud outweighed the penalties from getting caught, signalling weak sentences being appropriated to identity fraudsters by the judicial system in New Zealand. However, despite calling for greater legislative penalties, the financial sector in New Zealand has felt a large amount of pressure placed upon them with the new *Anti-Money Laundering and Counter Financing of Terrorism Act 2009*, which places the onus of customer identification firmly on the industry. It was stated that this onus was “unfair”, suggesting that the private sector does not have a sufficient public sector support framework in order to successfully identify customers.

In order for New Zealand to successfully fight identity fraud, the New Zealand Government needs to implement the basics correctly. Recommendations are as follows:

1. Principle 11(e)(i) of the *Privacy Act 1993* should be a sufficient basis for *all* public sector agencies to share information relating to suspected identity fraud cases. This Principle states that non-compliance is necessary:

To avoid prejudice to the maintenance of the law by any public sector agency, including the prevention, detection, investigation, prosecution, and punishment of offences;

2. A commitment from the upper echelons of government to close any loopholes in any system that facilitates identity fraud. Working in a proactive, rather than a reactive manner and recognising that any potentiality for identity fraud is a problem.

3. Analysis of statistics is conducted to build an intelligence profile and cost analysis and is distributed on a regular basis to public and private sector organisations.
4. Identity fraud based outcomes and the relevant outputs are developed and implemented into all organisations that interact with the public for goods or services.
5. Various Acts are synergised in terms of identity fraud legislative provisions to prevent identity fraudsters from evading punishment under certain Acts.
6. Cross-jurisdictional legislation or co-operative agreements are developed with other countries, in order for offending that occurs offshore but against New Zealand documents or services to be dealt with in the judicial system.
7. Closing or severely limiting the open public access to personal information held on public registers in New Zealand.
8. Preventing any member of the public from gaining an individual's birth, death, marriage or name change certificate.
9. Strengthening the verification process to obtain a New Zealand driver's licence.
10. New Zealand needs to quickly implement an identity verification process (notwithstanding the fact that the new *Anti-Money Laundering and Counter-Financing of Terrorism Act* came into effect on October 15, 2009, placing the onus on the financial industry to verify the identity of customers).
11. The development of an identity fraud taskforce with multi-agency input and with a liaison function with the private sector.
12. Securing biometric capabilities for those public sector agencies that deliver high end products or services (for example, DIA, INZ, MSD).

13. The development of a specific identity fraud statute which could be applied across the public and private sectors. Once offences are defined and legislated under the one act, the collection of statistics and analysis of cost will be enabled.

14. The New Zealand Government acknowledges that identity fraud is a priority and that is backed up with the appropriate funding and resources.

Around the globe, countries rely on individuals to give them truthful information when applying for goods and services in which identity is a key component. In the absence of a global database of all of the world's citizens where each country's documents are impeccably secure, we are not ever going to render identity fraud extinct, but we must try to minimise the risk in our systems wherever possible. Committing an identity fraud offence poses little risk for big gains. Until New Zealand narrows the gap between risk and gain through the strengthening of systems capabilities and legislative penalties, identity fraud is going to maintain its popularity in the criminal world. The consequences of getting an identity wrong can be catastrophic. If New Zealand's systems fail to detect identity fraud and enable an act of terrorism or other transnational crimes to occur, the New Zealand Government would face international condemnation and political ramifications. Nonetheless, given that New Zealand has not even the basics securely in place in order to competently combat identity fraud at the present time, it is a long path ahead for the Government and one that is likely to span more than one term in office.

REFERENCES

- Alter, S. (2007). Could the work system method embrace systems concepts more fully? *Information Resource Management Journal*, 20(2), 33-43. Retrieved from http://www.usfca.edu/sobam/faculty/publications/alter_Could%20WSM%20Embrace%20Systems%20Concepts%20More%20Fully.pdf
- Alvesson, M., & Sköldbberg, K. (2000). *Reflexive methodology: New vistas for qualitative research*. London, UK: Sage.
- Anderson, K., Durbin, E., & Salinger, M. (2008). Identity theft. *Journal of Economic Perspectives*, 22(2), 171-192.
- Anti-Money Laundering and Countering Financing of Terrorism Act 2009*. Retrieved from <http://www.legislation.govt.nz/act/public/2009/0035/latest/096be8ed80482ff3.pdf>
- Anti-Money Laundering and Countering Financing of Terrorism Bill 2008*. Retrieved from <http://www.legislation.govt.nz/bill/government/2009/0046/latest/096be8ed80478c73.pdf>
- Archer, M. (2007). *Making our way through the world: Human reflexivity and social mobility*. Cambridge, UK: Cambridge University Press.
- Atkinson P., & Hammersley, M. (1994). Ethnography and participant observations. In N. Denzin & Y. Lincoln (Eds.), *Handbook of qualitative inquiry* (pp. 248-261). Thousand Oaks, CA: Sage.
- Auckland University of Technology postgraduate handbook 2009*. (2009). Auckland, New Zealand: University Postgraduate Centre, Author. Retrieved from http://www.aut.ac.nz/__data/assets/pdf_file/0005/60953/2009-postgraduate-handbook.pdf
- Australasian Centre for Policing Research. (2006). *Standardisation of definitions of identity crime terms: A step towards consistency* (Report series no. 145.3.). Payneham, South Australia: Author. Retrieved from http://www.acpr.gov.au/pdf/ACPR145_3.pdf
- Beardsley, A. (2004, March/April). Security in business and government. *Security OZ*, 28, 44-46. Retrieved from <http://www.securitysolutionsmagazine.com/Articles/SO28.pdf>
- Bennett, J. (2005). From ignorance to intervention: The role of Australia. In J. Henderson, & G. Watson (Eds.), *Securing a peaceful Pacific* (pp. 430-441). Christchurch, New Zealand: Canterbury University Press.
- Births, Deaths, Marriages and Relationships Registration (BDMRR) Amendment (BDMRR) Bill 98-1* 2007. Retrieved from <http://www.legislation.govt.nz/bill/government/2007/0098/5.0/096be8ed8013fe3b.pdf>
- Births, Deaths, Marriages and Relationships Registration (BDMRR) Act 2009*. Retrieved from <http://www.legislation.govt.nz/act/public/1995/0016/latest/096be8ed80349a98.pdf>
- Boa, K., Clement, A., & Hosein, G. (2006, November). *Challenges to a Canadian identity policy: Learning from international experiences*. Paper presented at the 7th Annual Privacy and Security Workshop & 15th CACR Information Security Workshop. [Powerpoint

presentation] Retrieved from
http://www.cacr.math.uwaterloo.ca/conferences/2006/psw/Clement.ppt#256,1,Challenges_to_a_Canadian_Identity_Policy

Boguslaw, R. (1982). *Systems analysis and social planning: Human problems of post-industrial society*. New York, NY: Irvington.

Border Sector Governance Group. (2008). *Border sector strategy: 2008-2013: A framework for collaboration for border sector agencies*. Retrieved from
<http://www.customs.govt.nz/NR/rdonlyres/A7B532AD-BEEB-4D3A-8BCE-01BA0015735E/0/BorderSectorStrategy20082013.pdf>

Brannen, J. (2004). Working qualitatively and quantitatively. In C. Seale, G. Gobo, J. Gubrium, & D. Silverman (Eds.), *Qualitative research practice* (pp. 282-296). Thousand Oaks, CA: Sage.

Brock, B., Chesebro, J., Cragan, J., & Klumpp, J. (1973). *Public policy decision-making: Systems analysis and comparative advantages debate*. New York, NY: Harper & Row.

Burnham, P., Gilland, K., Grant, W., & Layton-Henry, Z. (2004). *Research methods in politics*. Hampshire, UK: Palgrave MacMillan.

Canadian Internet Policy and Public Interest Clinic. (2007). *Identity theft: Introduction and background* (CIPPIC Working Paper No. 1 ID Theft Series). Retrieved from
<http://www.cippic.ca/documents/bulletins/Introduction.pdf>

Cast, A. (2003). Identities and behaviour. In P. Burke, T. Owens, R. Serpe, & P. Thoits (Eds.), *Advances in identity theory and research*. New York, NY: Kluwer.

Cheek, J. (2007). The practice and politics of funded qualitative research. In N. Denzin, & Y. Lincoln (Eds.), *Strategies of qualitative inquiry* (3rd ed., pp. 45-74). Thousand Oaks, CA: Sage.

Citizenship Act 1977. Retrieved from
<http://www.legislation.govt.nz/act/public/1977/0061/latest/096be8ed803490a5.pdf>

Considine, M. (1994). *Public policy: A critical approach*. South Melbourne, Australia: MacMillan.

Corti, L., & Thompson, P. (2004). *Secondary analysis of archived data*. In C. Seale, G. Gobo, J. Gubrium, & D. Silverman (Eds.), *Qualitative research practice* (pp. 327-343). Thousand Oaks, CA: Sage.

Council of Australian Governments. (2007). *An agreement to a national identity security strategy*. Retrieved from http://www.coag.gov.au/coag_meeting_outcomes/2007-04-13/docs/national_identity_security_strategy.pdf

Crimes Act 1961. Retrieved from
<http://www.legislation.govt.nz/act/public/1961/0043/latest/096be8ed80488ad9.pdf>

Crosby, J. (2008). *Challenges and opportunities in identity assurance*. Retrieved from

Davies, S., & Hosein, G. (2007). *Identity policy: Risks & rewards: Report prepared for the U.S. Federal Trade Commission*. Retrieved from
<http://www.ftc.gov/bcp/workshops/proofpositive/ftc-identity-final.pdf>

- Delamont, S. (2004). Ethnography and participant observation. In C. Seale, G. Gobo, J. Gubrium, & D. Silverman (Eds.), *Qualitative research practice* (pp. 217-229). Thousand Oaks, CA: Sage.
- Deloitte. (2006). *2006 Global security survey*. Retrieved from [http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/us_fsi_150606globalsecuritysurvey\(1\).pdf](http://www.deloitte.com/assets/Dcom-Shared%20Assets/Documents/us_fsi_150606globalsecuritysurvey(1).pdf)
- Dept of Labour v Ioasa* HC AK CRI-2008-404-000145 [11 August 2008]
- Easton, D. (1965). *A systems analysis of political life*. New York, NY: Wiley.
- FakeID*. (n.d.). Retrieved November 18, 2009 from <http://fakepassport.com>
- Financial Action Task Force. (2009). *Financial Action Task Force annual report 2008-2009*. Retrieved from <http://www.fatf-gafi.org/dataoecd/11/58/43384540.pdf>
- Finlay, L. (2003). *The reflexive journey: Mapping multiple routes*. In L. Finlay & B. Gough (Eds.), *Reflexivity: A practical guide for researchers in health and social sciences* (pp. 3-20). Oxford, UK: Blackwell.
- Goffman, E. (1990). *Stigma: Notes on the management of spoiled identity*. London, UK: Penguin.
- Gomm, R. (2004). *Social research methodology: A critical introduction*. Basingstoke, UK: Palgrave MacMillan.
- Gordon, G. & Willox, N. (2006). The ongoing critical threats created by identity fraud: An action plan. *Journal of Economic Crime Management*, 4(1), 1-15 Retrieved from <http://www.utica.edu/academic/institutes/ecii/publications/articles/E8F7F48E-9E15-5DB3-5AACFB8980A15EFF.pdf>
- Gough, B. (2003). *Deconstructing reflexivity*. In L. Finlay & B. Gough (Eds.), *Reflexivity: A practical guide for researchers in health and social sciences* (pp. 21-35). Oxford, UK: Blackwell.
- Hackers hit Shell. (2009, March 18). *Taranaki Daily News*, p. 3.
- Hesse-Biber, S., & Leavy, P. (2006). *The practice of qualitative research*. Thousand Oaks, CA: Sage.
- Hinde, A. (2002). *Secondary analysis*. In G. Allan & C. Skinner (Eds.), *Handbook for research students in the social sciences* (pp. 203-224). London, UK: Falmer.
- Home Office. (2006, December). *Borders, immigration and identity action plan: Using the National Identity Scheme to strengthen our borders and enforce compliance within the UK*. Retrieved from <http://ukba.homeoffice.gov.uk/sitecontent/documents/managingourborders/bordersimmigrationactionplan/bordersactionplan.pdf?view=Binary>
- Hoos, I. (1972). *Systems analysis in public policy: A critique*. Berkeley, CA: University of California Press.
- Hosein, G. (2008). Politics and identity management. In E. de Leeuw, S. Fischer-Hübner, J. Tseng, & J. Borking (Eds.), *Policies and research in identity management* (pp. 3-4). New York, NY: Springer.

- Immigration Act 1987*. Retrieved from <http://www.legislation.govt.nz/act/public/1987/0074/latest/096be8ed8025b157.pdf>
- Immigration Bill 132-2 (2007)*. Retrieved from <http://www.legislation.govt.nz/bill/government/2007/0132/24.0/096be8ed80245e53.pdf>
- International Civil Aviation Organization. (n.d.). *Annex 9*. Retrieved from <http://www2.icao.int/en/AVSEC/FAL/Pages/Annex9.aspx>
- International Monetary Fund, (2005). *New Zealand: Report on the observance of standards and codes: FATF recommendations for anti-money laundering and combating the financing of terrorism* (IMF Country Report No. 05/284). Retrieved from http://www.justice.govt.nz/policy-and-consultation/crime/documents/fatf/IMF-ROSC-for-NZ.pdf/at_download/file
- Interpol. (2008a). *Trafficking in human beings*. Retrieved from <http://www.interpol.com/Public/ICPO/FactSheets/THB02.pdf>
- Interpol. (2008b). *People smuggling*. Retrieved from <http://www.interpol.com/Public/ICPO/FactSheets/THB01.pdf>
- Jones, C. (2002). *Qualitative interviewing*. In G. Allan & C. Skinner (Eds.), *Handbook for research students in the social sciences* (pp. 203-224). London, UK: Falmer.
- Jorgensen, D. (1989). *Participant observation: A methodology for human studies*. Thousand Oaks, CA: Sage.
- Kelsey, J. (2001). *Secondary sources*. In C. Davidson, & M. Tolich (Eds.), *Social science research in New Zealand: Many paths to understanding* (2nd ed., pp. 309-315). Auckland, New Zealand: Pearson.
- Koops, B., Leenes, R., Meints, M., van der Meulen, N., & Jaquet-Chiffelle, D. (2009). A typology of identity-related crime: Conceptual, technical, and legal issues. *Information, Communication & Society*, 12(1), 1-24.
- KPMG, (2008). *Forensic fraud survey 2008*. Retrieved from <http://www.kpmg.com.au/Portals/0/Fraud%20Survey%202008.pdf>
- Krone, R. (1980). *Systems analysis and policy sciences*. New York, NY: John Wiley.
- Ladley, A., & White, N. (2006). *Conceptualising the border*. Wellington, New Zealand: Institute of Policy Studies, School of Government, Victoria University.
- Land Transport Amendment Bill (No 4)*. Retrieved from http://www.parliament.nz/NR/rdonlyres/056DEE64-C4F9-4979-B492-74A989839037/105200/DBHOH_BILL_8313_LandTransportAmendmentBillNo4_6379.pdf
- Land Transport New Zealand. (2006). *Statement of intent 2006-2009*. Retrieved from <http://www.ltsa.govt.nz/about/docs/statement-of-intent-2006-09.pdf>
- Land Transport New Zealand. (2007). *Annual report for the year ending 30 June 2007*. Retrieved from <http://www.ltsa.govt.nz/about/annual-report/2007/docs/annual-report-2007.pdf>

Lee v Dept of Labour HC AK CRI 2007-404-0126 [9 July 2007].

Maso, I. (2003). *Necessary subjectivity: Exploiting researchers' motives, passions and prejudices in pursuit of answering 'true' questions*. In L. Finlay & B. Gough (Eds.), *Reflexivity: A practical guide for researchers in health and social sciences* (pp. 39-51). Oxford, UK: Blackwell.

May, T. (2001). *Social research: Issues, methods and process* (3rd ed.). Buckingham, UK: Open University Press.

McAdams, D., Josselson, R., & Lieblich, A. (2006). Introduction. In D. McAdams, R. Josselson, & A. Lieblich (Eds.), *Identity and story: Creating self in story* (pp.3 – 11). Washington DC: American Psychological Association.

McMurray, A., Pace, R. W., & Scott, D. (2004). *Research: A commonsense approach*. South Bank, Australia: Thomson.

Ministry of Social Development v Wayne Thomas Patterson. HC AK CRI 2006-090-010420 [12 October 2007]

Miser, H., & Quade, E. (1985). The context, nature, and use of systems analysis. In H. Miser & E. Quade (Eds.), *Handbook of systems analysis: Overview of uses, procedures, applications, and practice* (pp. 1-38). New York, NY: Elsevier.

Model Criminal Law Officers' Committee of the Standing Committee of Attorneys-General, Model Criminal. (2008). *Final Report Identity Crime*. Retrieved from [http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/\(CFD7369FCAE9B8F32F341DBE097801FF\)~6Final+Report+Identity+Crime+March+2008.PDF/\\$file/6Final+Report+Identity+Crime+March+2008.PDF](http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(CFD7369FCAE9B8F32F341DBE097801FF)~6Final+Report+Identity+Crime+March+2008.PDF/$file/6Final+Report+Identity+Crime+March+2008.PDF)

Naím, M. (2006). *Illicit: How smugglers, traffickers, and copycats are hijacking the global economy*, London: UK: Heinemann.

New Zealand Customs Service. (2008). *Annual report 2007-2008*. Retrieved from <http://www.customs.govt.nz/library/Accountability+Documents/Annual+Report+2007-2008/Annual+Report+2007-2008.htm>

New Zealand Customs Service. (2009). *Statement of intent 2009-2012*. Retrieved from <http://www.customs.govt.nz/NR/rdonlyres/6B4D099D-071D-4D8D-BD7E-074886594D83/0/CustomsSOI20092012web.pdf>

New Zealand Department of Internal Affairs. (2006). *Evidence of identity standard*. Retrieved from [http://www.dia.govt.nz/diawebsite.nsf/Files/EOIStandard/\\$file/EOIStandard.pdf](http://www.dia.govt.nz/diawebsite.nsf/Files/EOIStandard/$file/EOIStandard.pdf)

New Zealand Department of Internal Affairs. (2007). *Statement of intent 2007-10*. Retrieved from [http://www.dia.govt.nz/Pubforms.nsf/URL/DIASOI2007-10-complete.pdf/\\$file/DIASOI2007-10-complete.pdf](http://www.dia.govt.nz/Pubforms.nsf/URL/DIASOI2007-10-complete.pdf/$file/DIASOI2007-10-complete.pdf)

New Zealand Department of Internal Affairs. (2008). *Annual report 2007-08*. Retrieved from [http://www.dia.govt.nz/pubforms.nsf/URL/DIAAnnReport08.pdf/\\$file/DIAAnnReport08.pdf](http://www.dia.govt.nz/pubforms.nsf/URL/DIAAnnReport08.pdf/$file/DIAAnnReport08.pdf)

New Zealand Department of Internal Affairs. (2009a). *Request for New Zealand birth certificate and/or birth printout* (BMD93B 03/09) [Brochure]. Retrieved from <http://www.dia.govt.nz/Pubforms.nsf/URL/BirthCertificateorPrintoutRequestForm.pdf>

- New Zealand Department of Internal Affairs. (2009b). *Name change by statutory declaration* (BDM120 09/09). [Brochure]. Retrieved from [http://www.dia.govt.nz/pubforms.nsf/URL/ChangeofNameBDM120.pdf/\\$file/ChangeofNameBDM120.pdf](http://www.dia.govt.nz/pubforms.nsf/URL/ChangeofNameBDM120.pdf/$file/ChangeofNameBDM120.pdf)
- New Zealand Department of Labour. (2008). *Annual report 2007/08: Department of Labour's annual report for the year ended 30 June 2008*. Retrieved from <http://www.dol.govt.nz/PDFs/annualreport0708.pdf>
- New Zealand Department of Labour. (2009). *Statement of intent 2009/10-2012/13*. Retrieved from <http://www.dol.govt.nz/PDFs/soi-2009.pdf>
- New Zealand Law Commission. (2008). *Public registers: Review of the law of privacy: Stage 2* (NZLC R 101). Retrieved from http://www.lawcom.govt.nz/UploadFiles/Publications/Publication_129_391_Public_registers_web_72.pdf
- New Zealand Ministry of Justice. (2009). *Organised crime strategy 2008-2009*. Retrieved from <http://www.justice.govt.nz/policy-and-consultation/crime/organised-crime/organised-crime-strategy-2008-2009>
- New Zealand Ministry of Social Development. (2008). *Annual report 2007/2008*. Retrieved from <http://www.msd.govt.nz/documents/about-msd-and-our-work/publications-resources/corporate/msd-annual-report-2007-08.pdf>
- New Zealand Ministry of Social Development. (2009). *Statement of intent 2009-2012*. Retrieved from <http://www.msd.govt.nz/documents/about-msd-and-our-work/publications-resources/corporate/statement-of-intent/2009/msd-soi-2009.pdf>
- New Zealand Office of the Auditor-General. (2007). *Department of Labour: Management of immigration identity fraud*. Retrieved from <http://www.oag.govt.nz/2007/immigration/docs/oag-immigration.pdf>
- New Zealand Parliamentary Debates. (2008, July 22). Births, Deaths, Marriages, and Relationships Registration Amendment Bill (no. 3). Vol. 648, p. 17298. Retrieved from <http://www.parliament.nz/en-NZ/PB/Debates/Debates/1/1/9>
- New Zealand Police. (2008a). *Annual report for the year ended 30 June 2008*. Retrieved from http://www.police.govt.nz/resources/2008/annual-report/16003_RNZPC_Ann%20Report-LR.pdf
- New Zealand Police. (2008b). *Statement of intent 2008/09-2010/11*. Retrieved from <http://www.police.govt.nz/resources/2008/statement-of-intent/statement-of-intent-2008.pdf>
- New Zealand State Services Commission. (2001). *State sector standards board report to the Minister of State Services on a draft statement of government expectations of the State Sector*. Retrieved from http://www.ssc.govt.nz/display/document.asp?docid=2330&pageno=2#P29_1346
- New Zealand Transport Agency. (2009, August). Factsheet 20: Identification for driver licensing. Retrieved from <http://www.itsa.govt.nz/factsheets/20.html>
- Newton, K. (2008, December 1). Ticketek customer data sent in error. *The Dominion Post*, p. A4.

- The 9/11 Commission Report. (2004). *Final report of the National Commission on Terrorist Attacks Upon the United States*. New York, NY: Norton. Retrieved from <http://govinfo.library.unt.edu/911/report/911Report.pdf>
- Organisation for Economic Co-operation and Development. (2009). *Online identity theft*. Paris, France: Author. Retrieved from <http://browse.oecdbookshop.org/oecd/pdfs/browseit/9309021E.PDF>
- Paget, F. (2007). *Identity theft*. Retrieved from http://www.mcafee.com/us/local_content/white_papers/wp_id_theft_en.pdf
- Passports Act 1992*. Retrieved from <http://www.legislation.govt.nz/act/public/1992/0092/latest/096be8ed80125ddd.pdf>
- Patton, M. Q. (1990). *Qualitative evaluation and research methods* (2nd ed.). Thousand Oaks, CA: Sage.
- Pontell, H. (2002). *"Pleased to meet you ... won't you guess my name?": Reducing identity fraud in the Australian tax system*. Paper presented to the Centre for Tax System Integrity, The Australian National University, Canberra, Australia. Retrieved from <http://ctsi.anu.edu.au/publications/taxpres/Pontell.pdf>
- Privacy Act 1993*. Retrieved from <http://www.legislation.govt.nz/act/public/1993/0028/latest/096be8ed804ab387.pdf>
- Quade, E. (1985). Predicting the consequences: Models and modeling. In H. Miser & E. Quade (Eds.), *Handbook of systems analysis: Overview of uses, procedures, applications, and practice* (pp. 191-218). New York, NY: Elsevier.
- Raab, C. D. (2008). Social and political dimensions of identity. In S. Fischer-Hübner, P. Duquenoy, A. Zuccato, & L. Martucci (Eds.), *The future of identity in the information society* (pp.3-19). New York, NY: Springer.
- Rapley, T. (2004). *Interviews*. In C. Seale, G. Gobo, J. Gubrium, & D. Silverman (Eds.), *Qualitative research practice* (pp. 15-33). London, UK: Sage.
- Robson, C. (2002). *Real world research: A resource for social scientists and practitioner-researchers* (2nd ed.). Oxford, UK: Blackwell.
- Savin-Baden, M. (2004). Achieving reflexivity: Moving researchers from analysis to interpretation in collaborative inquiry. *Journal of Social Work Practice*, 18(3), 365-378.
- Schutt, R. (2006). *Investigating the social world: The process and practice of research* (5th ed.). Thousand Oaks, CA: Sage.
- Skyttner, L. (2005). *General systems theory: Problems, perspectives, practice*. Hackensack, NJ: World Scientific.
- Smith, R. (2008). Coordinating individual and organisational responses to fraud. *Crime, Law and Social Change*, 49(5), 379-396.
- Soghoian, C. (2008). *Insecure flight: Broken boarding passes and ineffective terrorist watch lists*. In E. de Leeuw, S. Fischer-Hübner, J. Tseng, & J. Borking (Eds.), *Policies and research in identity management* (pp. 5-23). New York, NY: Springer.
- Spradley, J. (1979). *Participant observation*. New York, NY: Holt, Rinehart & Winston.

- Stewart, D. (1984). *Secondary research: Information sources and methods*. Thousand Oaks, CA: Sage.
- Stewart, J., & Ayres, R. (2001). Systems theory and policy practice: An exploration. *Policy Sciences*, 34(1), 79-94.
- Tagicakibau, E. (2005). *A Pacific conflict transformation network?* In J. Henderson & G. Watson (Eds.), *Securing a peaceful Pacific* (pp. 192-201). Christchurch, New Zealand: Canterbury University Press.
- Tax Administration Act 1994*. Retrieved from <http://www.legislation.govt.nz/act/public/1994/0166/latest/096be8ed80485d3d.pdf>
- Tolich, M., & Davidson, C. (1999). *Starting fieldwork: An introduction to qualitative research in New Zealand*. Auckland, New Zealand: Oxford University Press.
- Transparency International. (2006). *CPI Table 2006*. Retrieved from http://www.transparency.org/news_room/in_focus/2006/cpi_2006/cpi_table
- Unisys Security Index. (2009). *New Zealand April 2009 a consumer link survey* Retrieved from http://www.unisys.com.au/eprise/main/admin/country/doc/au/NZ_Security_Index_Apr_09_FINAL.pdf
- United Nations High Commissioner for Refugees. (1951). *Convention and protocol relating to the status of refugees*. Retrieved from <http://www.unhcr.org/protect/PROTECTION/3b66c2aa10.pdf>
- United States Department of the Treasury. (n.d.) Office of foreign assets control. Retrieved from <http://www.treas.gov/offices/enforcement/ofac/>
- United States General Accounting Office. (2002, February 14). *Identity theft: Available data indicate growth in prevalence and cost: Statement of Richard M. Stana, Director, Justice Issues, before the Subcommittee on Technology, Terrorism and Government Information, Committee on the Judiciary, U.S. Senate* (GAO-02-424-T). Retrieved from <http://www.gao.gov/new.items/d02424t.pdf>
- Victoria Ombudsman. (2007, December). *Investigation into VicRoads driver licensing arrangements*. Retrieved from http://www.ombudsman.vic.gov.au/resources/documents/Investigation_into_VicRoads_driver_licensing_arrangements.pdf
- Wayne Thomas Patterson v The Queen* [2008] NZSC 70. Retrieved from http://www.courtsofnz.govt.nz/cases/wayne-thomas-patterson-v-the-queen/at_download/fileDecision
- Whitley, E., & Hosein, I. (2008). Departmental influences on policy design. *Communications of the ACM*, 51(5), 98-100.
- Wishart, I. (1999). *The god factor*. Auckland: New Zealand: Howling at the Moon.

GLOSSARY

ALO: Airline Liaison Officer. ALOs are employed by immigration agencies in their respective countries to work at offshore ports.

AML: Anti-Money Laundering.

AMS: Application Management System.

APP: Advanced Passenger Processing.

BDM: Births, Deaths and Marriages.

Bio data: Personal identifying data such as name, date of birth, gender.

Biometric: A biologically related measure such as a fingerprint or iris scan.

BNZ: Bank of New Zealand.

Caption Sheet: A summary document of the charges that an offender has been charged with under legislation.

CFT: Combating or Counter-Terrorist Financing.

CIPPIC: Canadian Internet Policy and Public Interest Clinic

COAG: Council of Australian Governments.

DIA: Department of Internal Affairs.

DOL: Department of Labour.

DVS: Data Validation Service.

EOI: Evidence of Identity Standard.

FATF: Financial Action Task Force.

FSF: Financial Services Federation.

IAG: IAG Insurance.

IAS: Identity Assurance Strategy.

INZ: Immigration New Zealand.

IMF: International Monetary Fund.

IRD: Inland Revenue Department.

IVS: Identity Verification Service.

LTNZ: Land Transport New Zealand.

MAF: Ministry of Agriculture and Forestry.

MOT: Ministry of Transport.

MSD: Ministry of Social Development.

NIBRS: National Incident-Based Reporting System (United States of America).

NZCS: New Zealand Customs Service.

NZFSA: New Zealand Food Safety Authority.

NZP: New Zealand Police.

NZTA: New Zealand Transport Agency.

OAG: Office of the Auditor-General.

OECD: Organisation for Economic Co-operation and Development.

Permit: The New Zealand Government grants permits to people upon arrival in New Zealand (in some cases on the basis of a visa). A permit allows a person *to remain* in New Zealand for a certain period of time.

RMAL: Regional Movement Alert List. It is a database of reported lost and stolen New Zealand, Australian and United States passports. The database is shared between these countries.

SITA: The name of an information technology company that administers a messaging service for airlines.

SSC: State Services Commission.

Summary of Facts: A summary document of the circumstances against an offender that forms the basis for the offender being charged.

UCR: Uniform Crime Reports (United States of America).

UN IEG: United Nations Intergovernmental Expert Group.

Visa: The New Zealand Government grants visas to people to *travel to* New Zealand. Visas state how long a person may be granted a *permit* for to remain in New Zealand.

**APPENDIX A – Auckland University of Technology Ethics
Committee (AUTEC) Approval Memorandum**



M E M O R A N D U M

Auckland University of Technology Ethics Committee (AUTEC)

To: Marilyn Waring
 From: **Madeline Banda** Executive Secretary, AUTEC
 Date: 28 May 2007
 Subject: Ethics Application Number 07/64 **Am I who I say I am? A systems analysis into identity fraud in New Zealand.**

Dear Marilyn

I am pleased to advise that the Auckland University of Technology Ethics Committee (AUTEC) approved your ethics application at their meeting on 14 May 2007, subject to the following conditions:

1. Inclusion in the Consent Form of the information given in the responses to sections D.9 and D.10 of the application;
2. Clarification of the processes by which organisational consent, including permission for the disclosure of the organisation's identity in the findings, will be obtained;
3. Amendment of the Information Sheet by replacing the term 'anonymous' with the term 'confidential';
4. Clarification of the reference to obtaining police clearance in the Confidentiality Agreement.

I request that you provide the Ethics Coordinator with written evidence that you have satisfied the points raised in these conditions within six months. Once this evidence has been received and confirmed as satisfying the Committee's points, you will be notified of the full approval of your ethics application. If these conditions have not been satisfactorily met within six months, your application will be closed and you will need to submit a new application should you wish to continue with the research.

You may not of course commence research until full approval has been confirmed. You need to be aware that when approval has been given subject to conditions, full approval is not effective until *all* the concerns expressed in the conditions have been met to the satisfaction of the Committee.

To enable us to provide you with efficient service, we ask that you use the application number and study title in all written and verbal correspondence with us. Should you have any further enquiries regarding this matter, you are welcome to contact Charles Grinter, Ethics Coordinator, by email at charles.grinter@aut.ac.nz or by telephone on 921 9999 at extension 8860.

Yours sincerely

Madeline Banda
Executive Secretary
Auckland University of Technology Ethics Committee

Cc: Mireille Giaccherini mimigia@gmail.com

APPENDIX B – Participant Information Sheet

Participant Information Sheet



Date Information Sheet Produced:

20 August 2007

Project Title

Am I Who I Say I Am? A Systems Analysis into Identity Fraud in New Zealand

An Invitation

My name is Mireille Giaccherini and I am currently studying towards a Master of Philosophy degree. I am undertaking research for my thesis in the identity fraud field.

I have selected a number of people who I wish to interview in relation to identity fraud in New Zealand and I invite you to participate in this process. Your participation in this interview is voluntary and you may withdraw at any time, prior to the collation of data, without prejudice.

What is the purpose of this research?

The purpose of this research is to conduct a systems analysis into identity fraud in New Zealand. I intend to explore the current identification procedures operating at an organisational level in the context of best practice parameters and legislative requirements. In addition, I will research current and emerging trends in identity fraud, as well as examining the environmental impacts on identity verification in New Zealand.

The final research findings will be published in a master's thesis and will be publicly available. A summary of my thesis will be available to you upon request.

How was I chosen for this invitation?

Initially I selected organisations who deal with identity crimes on a regular basis. Subsequently, I identified the business unit(s) within each organisation who investigate, prosecute or develop policies in their respective areas. You have been selected to be interviewed based upon your knowledge of identity related issues.

What will happen in this research?

I intend to conduct an interview with you that will take approximately one hour. Some of the questions that I will ask will be standard questions that will also be asked of other interviewees; however, there will be opportunity to ask any additional questions. The interview will be audio-taped and transcribed by a third party, who will hold the appropriate

police clearance. I will also take brief notes during the interview. Once the interview has been transcribed, I will send a hard copy to you for your review.

What are the discomforts and risks and how will they be mitigated?

I do not anticipate that there will be any discomfort in the interview process.

In terms of ethical risk, it is important to give due consideration to any information that may security classified. I do not intend to ask any questions that may lead to the disclosure of any information pertaining to national security. With this in mind, I will send you a copy of the transcribed interview for your review.

In writing my research findings, I would like to identify both yourself and the organisation that you work for. However, if you wish your details to be kept confidential in the research findings, I will allocate you a pseudonym so that you cannot be identified.

If you are the person who is giving organisational consent and one of your employees requests their details to remain confidential in the research findings, the organisation will also be allocated a pseudonym to protect the identity of the employee.

Maintaining the privacy of any individual (for example, in a case or investigation) is imperative. Therefore, I will not include the biodata of any person in my thesis that is currently under investigation or in the judicial system.

All files, including interview transcripts and audiotapes will be stored in a secure cabinet in my supervisor's office at AUT. Moreover, any third party employed such as a transcriber, will be required to sign a confidentiality agreement and hold the appropriate police clearance.

What are the benefits?

The benefits of this research are three-fold. Firstly, it will improve my research skills and knowledge. Secondly, it will provide me with a greater understanding of identity verification practices and the associated environmental impacts. Thirdly, I hope that the research findings will assist in future policy-making in the identity field. In this vein, the benefits will extend to the community, both in aiding understanding of identity fraud as well as raising awareness to combat the problem.

What are the costs of participating in this research?

The only envisaged cost is for you to spend approximately one hour of your time being interviewed.

What opportunity do I have to consider this invitation?

Please notify me within ten working days of receiving this information sheet, should you be willing to participate in my research. I will subsequently contact you directly to confirm an interview date and time.

How do I agree to participate in this research?

I have enclosed a consent form for you to read, sign and return to me if you agree to participate in this research.

Will I receive feedback on the results of this research?

I am willing to provide you with a summary of my thesis, at the completion of my degree, upon request.

What do I do if I have concerns about this research?

Any concerns regarding the nature of this project should be notified in the first instance to the Project Supervisor, Professor Marilyn Waring, Marilyn.Waring@aut.ac.nz, phone 09 921 9661.

Concerns regarding the conduct of the research should be notified to the Executive Secretary, AUTEK, Madeline Banda, madeline.banda@aut.ac.nz, 09 921 9999 ext 8044.

Whom do I contact for further information about this research?

Researcher Contact Details:

Should you wish to contact me for any further information in relation to this research, please email me at the following address: mimigia@gmail.com.

Project Supervisor Contact Details:

Professor Marilyn Waring
Institute of Public Policy
Auckland University of Technology
PO Box 92006
AUCKLAND
Email: Marilyn.Waring@aut.ac.nz
Phone: 09 921 9661

Approved by the Auckland University of Technology Ethics Committee on 17 August 2007, AUTEK Reference number 07/64.