Association for Information Systems
AIS Electronic Library (AISeL)

ACIS 2008 Proceedings | Australasian (ACIS)

2008

Defining Identity Crimes

Rodger Jamieson
School of Information Systems, Technology, and Management University of New South Wales Sydney, Australia, r.jamieson@unsw.edu.au

Lesley Land
School of Information Systems, Technology, and Management University of New South Wales Sydney, Australia, l.land@unsw.edu.au

Rick Sarre
School of Commerce University of South Australia Adelaide, Australia, Rick.Sarre@unisa.edu.au

Alex Steel
Faculty of Law, UNSW, a.steel@unsw.edu.au

Greg Stephens
School of Information Systems, Technology, and Management University of New South Wales Sydney, Australia, g.stephens@unsw.edu.au

See next page for additional authors

Authors
Rodger Jamieson, Lesley Land, Rick Sarre, Alex Steel, Greg Stephens, and Donald Winchester

Defining Identity Crimes

Rodger Jamieson
Lesley Land
School of Information Systems, Technology, and Management
University of New South Wales
Sydney, Australia
Email: (r.jamieson, l.land)@unsw.edu.au

Rick Sarre
School of Commerce
University of South Australia
Adelaide, Australia
Email: Rick.Sarre@unisa.edu.au

Alex Steel
Faculty of Law, UNSW

Greg Stephens
Donald Winchester
School of Information Systems, Technology, and Management
University of New South Wales
Sydney, Australia
Email: (a.steel, g.stephens, d.winchester)@unsw.edu.au)

Abstract

The objective of this paper is to report on the definitions of the terms used and in use across different regions for identity crime, namely, identity fraud, identity theft, and identity deception. The purpose is to clarify the meaning of the terms used with a view to gaining a consensus amongst the various stakeholders. This consensus is essential to enable further research. Without consensus measurement and comparisons are meaningless. Our study of identity fraud has an industry-driven research agenda. A grounded theory research methodology is used when interviewing government agencies and private organisation participants. Interviews sought to better understand current information and communications technology (ICT) practitioners' security and privacy issues with respect to identity fraud perpetrator attacks. We found there to be consensus among stakeholders for the meaning of identity fraud and identity theft but less agreement for identity deception.

Keywords

Information and communications technology (ICT) security and privacy, identity crime definitions, identity fraud, identity theft, identity deception

INTRODUCTION

> *"… so it's all about definitions if you want to truly get an indication of the quantity … the extent of this particular activity (Identity Fraud) … it's also about the people collecting that information … and how they classify it"* (Participant 3)

Government agencies and private organisations the world over are increasingly delivering services electronically to save costs and improve effectiveness and efficiency. Integral to this is increased reliance on technological forms of identity verification which overcome the need for face-to-face verification. Ironically, this reliance has increased the possibility of identity crime.

Definitions in this field are important. An often cited problem for identity crime research is definitional issues regarding the meaning of the terms, identity fraud, identity theft or identity deception for data collection, data analysis, and comparison among results (Australian Centre for Policing Research (ACPR) 2006; ACPR 2004; Cheney 2005; Cuganesan and Lacey 2003; Jamieson et al. 2008; Le Lievre and Jamieson 2005; Model Criminal Law Officers' Committee (MCLOC) 2008; MCLOC 2007; Newman and McNally 2005; Wang et al. 2004). The Home Office Identity Fraud Steering Committee (2004, p. 1) is a very useful start. It clarifies that identity crime as "a generic term for identity theft, creating a false identity or committing identity fraud. False identity is:

- a fictitious (invented) identity; or
- an existing (genuine) identity that has been altered to create a fictitious identity."

While an individual's identity is a complex and changing subjective notion (Finch 2003), identity crime centres on misuse of the relatively permanent set of identifiers that go to make up a person's legal identity. Identity crime involves the illegal use of any part of three components, of an individual's (and entity's) identity. The three components comprise biometric, attributed and biographical attributes:

1. Biometric identity – attributes that are unique to an individual - fingerprints, retina, voice, facial structure, DNA profile, hand geometry, heat radiation, and signature.
2. Attributed identity – comprise the components of an individual's identity that are given at birth - their full name, date and place of birth, parents' names, occupations, and addresses.
3. Biographical identity – contains life events and interactions with society that are built up over time - registration of birth, education enrolment and qualifications, electoral roll registration, details of benefits claimed and taxes paid, employment history, registration of marriage or divorce, name change, real property transactions and interactions with financial institutions, utility organisations, public authorities, and other government agencies.

The emerging literature on identity fraud gives contradictory views of its incidence level in terms of costs, victimisation and occurrence rates in surveys and research within and across countries. Because identity crimes largely fall within pre-existing general fraud offences, the legal system has been slow to appreciate the breadth and complexity of the forms of wrongdoing that can be perpetrated by means of false identities. While legal systems search for general descriptions that can capture all forms of fraud, industry requires more specific methodology and phenomenon based definitions of identity crime. This paper argues that with improvements and wider stakeholder consensus in identity crime terms there will be better collection, analysis and management of the identity fraud data and the dissemination of information and knowledge from subsequent data analysis.

From an industry-centric perspective, organisations face difficulties in establishing the identity of customers from online identifiers. Several current and prospective features of information, communications, and technology (ICT) have facilitated technology-enabled crime. These include:

- ICT becoming intrinsically connected to daily personal and organisational life,
- computer systems and networks that facilitate commercial and private use, but also create risks of subsequent exploitation by identity crime perpetrators,
- computer data that are intrinsically hard to control, especially with the ubiquity of the Internet which was designed to resist outside attempts to control its content or fields of operation,
- computer networks that are global, with information flowing via a number of networks and through a number of jurisdictions, and
- computers and computer networks that process and disseminate data extremely quickly (Council of Europe 2004).

Another issue, which has its roots in definitions of identity crime terms or categories, raised by interviewees (see methodology section for selection and experience) in this study and industry participants in general is the confusion over the quantum of identity fraud in Australia and other countries where different organisations have determined the cost (Canada, UK, US). For example the Australian Federal Police have estimated that identity crimes, such as money laundering, cost anywhere between $1 billion and $4 billion in Australia (Cass 2005, p.1). Similar disparities in the quantum are observed in the UK (McCue 2006) and the US (Newman and McNally 2005) and the basis of the estimates has been questioned (Ford and Charter 2006; Jamieson et al. 2008).

This topic also has implications for privacy law, since most attempts to address identity crime involve some inroads into privacy. The balance between these conflicting objectives is therefore important for both privacy and identity crime (Australian Law Reform Commission (ALRC) 2007; Crompton 2004).

It is also worth noting that not only does identity crime directly hurt victims, but it indirectly is an enabler of other criminal activity, such as e-crime (or electronic crime, a general term used to classify the investigation of criminal offences, where information systems, computers or other electronic devices have been used in some way to facilitate the commission of an offence), money laundering, terrorism financing and people smuggling (Choo et al. 2007). In addition there are many and varied, tried and true methods employed by identity crime perpetrators (such as, phishing, skimming, or hacking) and hence any activity to drive away the scourge needs to be multifaceted and cannot assume a 'one size fits all' response (Urbas and Choo 2008).

Prior research has noted shortcomings in earlier identity crime studies (Le Lievre and Jamieson 2005). The next section provides a literature review. The following sections describe the research methodology and discuss identity crime definitions from the literature and interviews. The last section concludes.

LITERATURE REVIEW

The importance of information systems (IS) security and privacy in organisations is well documented (Conway et al. 1972; Dhillon and Backhouse 2000; Karat et al. 2005; Straub 1990). However, IS research into ICT security is sparse (Mahmood et al. 2008). Research to date has been technically motivated (Straub et al. 2008), investigated breaches (Bagchi and Udo 2003; Gordon and Loeb 2002; Hinde 2002; Thompson 1998), developed security models (Straub and Welke 1998), and conducted literature surveys (Siponen and Willison 2007). But more IS security research is needed (Mahmood et al. 2008). One area of IS security attracting attention is identity crime methods often referred to as identity fraud, identity theft and identity deception or false identity, assumed identity, fictitious identity, identity fabrication, synthetic identity fraud, manipulated identity, counterfeit identity and impersonation fraud.

Although fraud involving assumed or false identities is probably as old as organised society, ICT has enabled both manipulation of automated services and deception from remote locations on a scale previously unimagined. While most frauds using false identities are adequately covered by general fraud and false instrument (forgery) laws, debate continues about whether specific identity crimes should be enacted to catch activities connected with activities prior to any fraud (Brown, et al. 2006; MCLOC 2007). Currently, in Australia, the Commonwealth (Part 10.8 *Criminal Code Act 1995* (Cth)), Queensland (s 408D *Criminal Code Act 1899* (Qld)) and South Australian (ss 144B- 144D *Criminal Law Consolidation Act 1935* (SA)) jurisdictions have offences that specifically prohibit the possession and use of false identities. However the vast bulk of identity crime appears to be prosecuted under general fraud laws, with obvious implications for the gathering and categorisation of statistics relating to identity fraud. To December 2007, there had only been seven convictions under the Commonwealth identity offences (Judicial Commission of NSW 2008). Models and conceptual frameworks for identity fraud are emerging and have been developed broadly on themes that have investigated costs (Cuganesan and Lacey 2003; Newman and McNally 2005; Home Office 2006; US Government Accounting Office (GAO) 2002; US GAO 1998), profiling (Le Lievre and Jamieson 2005), processes (Main and Robson 2001; Jamieson et al. 2007a) and definitions (ACPR 2006; ACPR 2004; ACPR 2000; Cheney 2005; Meulen 2006; MCLOC 2008; Sproule and Archer 2006; Wang et al. 2004).

The literature definitions of identity crime terms have developed geographically. Studies in the United States (US) have used the term identity theft most frequently (Cheney 2005; US GAO 2002; US GAO 1998). In the United Kingdom, Canada, and Australia clear distinctions were made between identity theft and identity fraud (in the UK: The Association for Payment Clearing Services (APACS) 2005; in Australia: ACPR 2006; ACPR 2004; ACPR 2000; Cuganesan and Lacey 2003; Le Lievre and Jamieson 2005; Main and Robson 2001; MCLOC 2008; MCLOC 2007; and in Canada: Office of the Privacy Commissioner of Canada 2007). "The lack of a standard definition makes it difficult to collect comprehensive, accurate data for quantifying the costs and incidents of identity theft." (United States Department of Treasury 2005, p. 9). The objective of our paper is to provide a standard definition.

METHODOLOGY

We use a method of grounded theory to investigate how identity crime terms shape organisational actions for improving information systems security when informed by privacy restrictions. We draw out themes from the interview data collected. The principles and procedures for data analysis prescribed by the Straussian approach (Corbin and Strauss 1990) were employed in this study. This approach was adopted due to its ability to systematically guide researchers.

This research involves a multi-method approach including the use of industry and government-based cross-sectional participant interviews (Interviewee quotes are in italics) and literature 'key word' searches of library, Internet, and proprietary databases using terms such as, identity crime, identity fraud, identity theft, and identity deception or synonyms. Interviewees represented banks, licensing authorities, government agencies (welfare, immigration), telecommunications and a US academic/criminologist (see Jamieson et al. 2007b, refer Table 1). Interviewee organisations were members of the AUSTRAC Identity Fraud Steering Committee. Interviewees held senior positions in fraud, fraud management, compliance, and/or internal audit. Our qualitative research empirical data was coded from interview transcripts. Data obtained from secondary sources, such as, supporting organisational, industry or sector documentation enabled the discovery of more detailed and refined concepts during grounded theory analysis (Corbin and Strauss 1990).

The main method of data collection employed in the study was a series of 12 semi-structured interviews. Some of the interviewees were previously employed in law enforcement or the legal profession. Each interview lasted approximately one and a half hours. Interviews were face-to-face except for two interstate interviews held by teleconference. The organisations represented are the most targeted by identity fraud perpetrators (Kim 2007).

Interviewee recordings were professionally transcribed and checked by an interviewer for accuracy. Transcripts were then coded into themes using 'key words' with qualitative analysis software (QSR NVivo 2005). The main key words used were; identity crime, identity fraud, identity theft, and identity deception. Relevant secondary data sources were also analysed. This included documentation on identity theft legislation.

IDENTITY CRIME DEFINITIONS

In this section we discuss the emergent definitions used in identity crime. A complicating factor in defining identity crime categories is that lawful use and creation of identities is intimately bound up in a jurisdiction's social, cultural and historical norms. Illegal uses of these identities are often merely seen as methodologies within already defined crimes. As a conceptually novel offence, identity crime and its categories differs from jurisdiction to jurisdiction providing an avenue for perpetrators to base their operations in jurisdictions offering little or no legal prohibitions on their activities; thus enabling them to take advantage of the confusion.

United States legislators led the way in defining identity crime as a separate criminal category when they made identity theft a national crime with the introduction of the Identity Theft and Assumption Deterrence Act of 1998 (ITADA, Public Law 105-318 - October. 30, 1998, see Table 1). The ITADA of 1998 makes the theft of personal information with the intent to commit an unlawful act a federal crime in the US, with penalties up to fifteen years imprisonment and a maximum fine of $250,000. In 1996, Arizona was the first US state to make identity theft a crime. Other state governments in the US have also prohibited identity theft, using a definition of identity theft that is substantially similar to that found in ITADA. Identity theft, as prohibited in ITADA and the state equivalents, is limited to the use of the "[m]eans of identification of another person." This focus on the use of a real person's identifiers is sometimes referred to as 'true person fraud'. The term has its origins in the harm that the statute intends to proscribe, that is, to an existing person, whose identity is assumed by the identity thief (Newman and McNally 2005; Willox and Regan 2002, p. 4).

However, today identity crime is conceived more broadly to include both true and fictitious identities. Thus in 2008 the Model Criminal Law Officers' Committee (MCLOC, p.16) recommended that all Australian jurisdictions enact legislation prohibiting the possession of identification information (other than their own) with intent to facilitate an indictable offence (see Table 2). Identification information is "information relating to a person (whether living or dead, real or fictitious, or an individual or body corporate) that is capable of being used (whether alone or in conjunction with other information) to identify or purportedly identify the person."

Table 1. Examples of Identity Theft Definitions Over Time and Across Regions

Author	Region	Definitions of Identity Theft
ITADA, Public Law 105-318 - October. 30, 1998	US	An identity thief is anyone who "[k]nowingly transfers or uses, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law."
Fair and Accurate Credit Trans-actions Act, 2003	US	Identity theft is "a fraud committed using the identifying information of another person", subject to such further definition as the FTC may prescribe, by regulation (15 U.S.C. §1681a(q)(3)) (also see Cheney, 2005; Meulen, 2006).
Home Office 2004	UK	Identity theft occurs when your personal information is used by someone else without your knowledge. It may support criminal activity, which could involve fraud, deception, or obtaining benefits and services in your name
CIFAS Online 2006	UK	Identity theft (also known as impersonation fraud) is the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity details are then used to obtain goods and services in that person's name
Office of the Privacy Commissioner of Canada 2007	Canada	Identity theft – or perhaps more accurately, identity fraud – occurs when someone uses your personal information, your Social Insurance Number (SIN) or birth date, for example, to pose as you and then apply for credit cards and loans, open bank accounts to write bad cheques and to get new government documents such as driver's licences and SIN cards

Indeed, there is also concern that proof of intent to commit a subsequent offence is overly difficult to establish and in some jurisdictions the scope of identity crime has expanded to include the mere possession of false identities. Thus s480.4 *Criminal Code Act 1995* (Cth) makes it an offence to obtain another's personal financial information dishonestly, and without consent.

Reaching agreement on a conceptual definition of identity fraud has, to date, proven naive as the identity crime phenomenon is continuously evolving (Cuganesan and Lacey 2003). For example, an earlier definition, posited by Main and Robson (2001, p. 1), described identity fraud "as an individual falsely representing him or herself as either another person to an organisation for some benefit" where "this misrepresentation is supported by fraudulently obtaining or falsely reproducing identity documents." Main and Robson's (2001) definition, while not globally accepted, provides a first principles interpretation and initiated ongoing debate, at least in Australia, about the scope that a definition for identity fraud should or should not encompass. This earlier debate on the typology was frustrated by the blurring of boundaries between country specific definitions of identity theft in the US and identity fraud in the UK, Canada, and Australia.

There is now an emerging literature that would suggest that there is some agreement on the fact that the crime of identity theft is a subset of identity fraud crimes and that the two terms preferably should not be used interchangeably to mean or refer to exactly the same crime in all situations (Porter 2004). To some extent this has been brought about by media reports (and the later categorisation of these crimes by academics and industry practitioners) of data on individuals/entity's identities being stolen (identity theft) from data repositories of entities across a wide range of sectors and of varying size. This stolen identity data (individuals' attributed and biographical information) was then used without the individuals' knowledge by the initial or subsequent perpetrators (identity thieves) for their criminal economic and/or financial gain (identity fraud). In Australia, government and law enforcement have now agreed on the following standard terminology shown in Table 2.

Table 2. Standard Identity Crime Terminology used by Australia Government

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

Source: Council of Australian Governments Agreement to a National Identity Security Strategy 2007, p. 3.

Table 3. Definitions of Identity Fraud across Regions and Time

Author	**Region**	**Definitions of Identity Fraud**
GAO 1998	US	Generally, identity fraud involves "stealing" another person's personal identifying information, for example, Social Security number, date of birth, and mother's maiden name. Criminals use such information to fraudulently establish credit, run up debt, or to take over existing financial accounts.
Cabinet Office 2002	UK	Identity fraud arises when someone takes over a totally fictitious name or adopts the name of another person with or without their consent.
ACPR 2004	Australia	Identity fraud refers to the gaining of money, goods, services or other benefits through the use of a false identity
CIFAS 2006	UK	Identity fraud is the use of a misappropriated identity in criminal activity, to obtain goods or services by deception. This usually involves the use of stolen or forged identity documents such as a passport or driving licence
Office of the Privacy Commissioner of Canada 2007	Canada	identity fraud – occurs when someone uses your personal information, your Social Insurance Number (SIN) or birth date, for example, to pose as you and then apply for credit cards and loans, open bank accounts to write bad cheques and to get new government documents such as driver's licences and SIN cards

It is not known however if these definitions are in use or useful to industry. Indeed the explosive growth of identity based fraud has led to some academics and industry participants, seeking to situate identity fraud universally, proposing narrower more prescriptive definitions.

The definitions in Table 1 and Table 3 demonstrate the confusing nature of definitions that have evolved in different countries and highlight the point made here that this difference hinders the regulation, data collection, and management or mitigation (prevention, detection, deterrence, and response) of this type of crime. Participants we interviewed predominantly define identity fraud from their own organisations, systems and processes' perspectives.

Prior to 1998 there were few specific statutes governing or very loose statutes governing identity crimes such as identity theft, identity deception, or identity fraud. Those statutes have been amended and tightened up or new legislation enacted so now doing certain forms of identity fraud are certainly crimes in themselves. But if you have someone's personal information and do nothing with it, that may not be a crime in some jurisdictions. Similarly, using a pseudonym, alias, stage name or pen name is mostly not an offence in itself. Identity fraud could be enabled by impersonating someone else or with false information thus entering an identification authentication or verification system is enabled via a stolen identity (identity theft) or a created identity (identity deception).

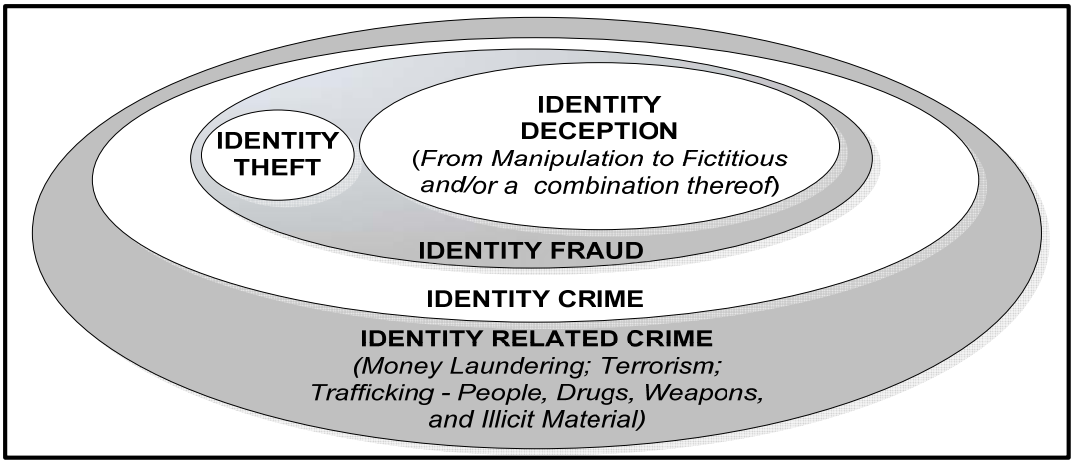

Figure 1. Conceptual Model of Identity Definitions

There is a need to create some type of typology of identity frauds because there are new forms emerging all the time. The term now refers to so many things that even if government or legislation in a jurisdiction is made current it soon becomes out of date" (Participant 12). This quotation illustrates the need for an accurate definition of identity crime delineating categories, such as identity fraud, identity theft and identity deception. Given the strong interrelation with traditional forms of fraud, and different approaches to the description of crime, legal definitions may be an unreliable basis on which to attempt to categorise the phenomenon. While some jurisdictions may favour a large number of specific offences, in other jurisdictions there is a clear trend toward generalised offences. This suggests that what is needed is a typology that is independent of the approaches to criminalisation used in legal systems..

The urgency to define and criminalise identity crimes stems from 'identity fraud', 'identity theft' and 'identity deception' being intertwined with the often related crimes of money laundering, terrorist financing, or trafficking in people, drugs, illicit material, and weapons, which impact communities in devastating ways (Cabinet Office 2002; Simon 2008; Sproule and Archer 2006). Identity fraud encompasses a continuum which includes 'identity theft' and 'identity deception' acts or events. Identity deception is a broader concept than identity theft (stolen identity details) because impersonation is just one of many ways to alter an identity (Wang et al. 2004). In the model presented as Figure 1, Identity Theft and Identity Deception have been separated. These activities or events are a precursor to the actual Identity Fraud; Identity Theft and/or Identity Deception must occur prior to the perpetrator committing Identity Fraud. Our proposal, as presented in the model suggests that Identity Theft, Identity Deception and Identity Fraud are the components of Identity Crime. As can be seen in the model there are also a considerable number of other related crimes that can result from identity crime.

What industry participants reiterated was that what identity crime requires is the actual adoption (misrepresentation) or use of someone else's identity in order to (intent) commit the fraud. Where financial institutions, specifically banks, mainly see identity fraud is in the false applications for credit cards and accounts. They also suggest that this is easy to measure. However, there are also some elements of identity fraud with cheque products which are far more complex. For example, perpetrators may establish a false business and then open up accounts. Consequently, future definitions of identity crime terms must go beyond individuals and include organisations or entities of all types. This is particularly important for rigorous data collection purposes.

Participant 3 states, *"there is some use in defining or distinguishing between identity theft and identity takeover (identity deception), where a person has been in fact made up, if you like fictitious, using false identification documentation."* The participant also indicated that it is easier to perpetrate an identity takeover where information is obtained through social engineering of the service environment; manipulation of call centre staff for example.

Government departmental definitions of identity fraud are usually informed by government regulation, legislation or mandated rules, or guidelines. Each of the identity crime categories identified by some government departments was approached in a different way because they manifest themselves differently. If the identity does not exist, there is no supporting evidence that can be found in other databases – births or marriages, immigration, education, employment, tax, or drivers licence. The only place that the identity will appear is on the proof of identity presented by the perpetrator. Instances were also discussed whereby a perpetrator could create another identity under a different name by transposing letters in a first or last name or changing an Asian name to an English name, for example (identity deception). In administration a typographical error on some document provides a perpetrator with the opportunity to start representing that altered name as their own. These instances are harder to detect, but basically they are still fictitious, created identities. Inaccuracies with data collected (when there is so much disparity in the definitions) render comparative analysis useless.

Table 4. Identity Crime Definitions Typology.

	Who is involved	**What is used**	**How it is committed**	**Purpose or Intent**
Identity Theft	Victim (individual or entity) Perpetrator (individual or organised crime)	True Identity Created Identity	Theft of wallet or purse, mail theft or redirection, dumpster diving, social engineering, phishing, and other evolving methods.	To commit Identity fraud or related crimes by: • Avoid detection • Anonymity • Shifting blame
Identity Deception	Perpetrator (individual of organised crime) Victim (sometimes)	Created Identity – from manipulated to fictitious or a mix thereof	Deceit through changes to actual data - change name, change initials, change residency details, change date of birth. (Wang et al. 2004)	
Identity Fraud	Victims (Individuals or entities) Perpetrators (Organised crime or individuals)	True Identity Created Identity	Apply for: Credit, Welfare, Loans, Purchase assets	Financial gain Avoid loss Money laundering Trafficking Terrorism

After discussions with participants and based on our typology in Table 4, we have developed some initial working definitions. These are set out below:

Identity Crime is a generic term for all identity fraud, identity theft, and identity deception acts (which ranges from manipulation to creation of fictitious identity details), and enables some related identity crimes.

Identity Theft happens when a perpetrator steals personal identifying information (individual or entity) to facilitate identity fraud or related identity crimes, irrespective of whether, the victim is living or deceased (or fictitious).

Identity Deception is a fictitious (i.e., invented) identity; or an existing (i.e., real – of a living or dead individual or entity; also includes lent identity documents or details) identity that has been altered to create a fictitious identity (individual or entity).

Identity Fraud is crystallised when identity details of an individual or entity obtained via theft or deceptive means are used to avoid an obligation or liability or misrepresent with intent.

Identity Related Crimes include using identity details of an individual or entity obtained via theft or deceptive means for money laundering, terrorism, trafficking – people, weapons, drugs or illicit material. Note an act or event is only a 'crime' if legislation is enacted.

These definitions will be the subject of further review and refinement but provide an initial point of discussion for further research into this area.

CONCLUSIONS

This study has demonstrated that industry groups have developed taxonomies of identity crime that are specific and useful to that industry group. This research used a typology to group the identity crime terms and we offer our working definitions of the categorised forms. What is clear, however, is that there is a need to delineate and capture data on the various methods by which stolen and deceptive identities are generated and used in addition to concentrating on the end use to which the identities are put (identity fraud, money laundering, terrorism, or trafficking in people, drugs, weapons or illicit material).

Private organisations interviewed saw identity fraud, identity theft and identity deception acts in much narrower focused terms than government agencies. Australian Federal and State agencies, while in some cases adopting their own internal meaning for the various identity crime terms, often had a broader definition for the identity crime terms prescribed by central government. This could have been driven from whole of government initiatives for defining identity crime (ACPR 2006; ACPR 2004; ACPR 2000). Our typology and working definitions were informed and grounded from the literature and interviews from industry and government experts with Australian and international expertise.

REFERENCES

The Association for Payment Clearing Services (APACS). 2005. "Card Fraud - The Facts: The definitive guide for the media on plastic card fraud and measures to prevent it," The Association for Payment Clearing Services, April, pp 1-34.

Australian Law Reform Commission (ALRC). 2007. "Review of Australian Privacy Law," Australian Government, Discussion Paper, (72), pp 1-1995.

Australian Centre for Policing Research (ACPR). 2006. "Standardisation of Definitions of Identity Crime Terms: A step towards consistency," Commonwealth of Australia, March, pp 1-22.

Australian Centre for Policing Research. 2004. "Standardisation of Definitions of Identity Crime Terms," Commonwealth of Australia, Discussion Paper, May, pp 1-8.

Australian Centre for Policing Research. 2000. "The Virtual Horizon: Meeting the Law Enforcement Challenges. Developing an Australasian law enforcement strategy for dealing with electronic crime," Scoping Paper. Australian Centre for Policing Research, (134.1), Adelaide, pp 1-185.

Bagchi, K., and Udo, G. 2003. "An Analysis of the Growth of Computer and Internet Security Breaches," *Communications of AIS*, (12), pp 684-700.

Brown, D., Farrier, D., Egger, S., McNamara, L., and Steel, A. 2006. Criminal Laws: Materials and commentary on criminal law and process in NSW. (4th ed), Federation Press, Australia.

Cabinet Office. 2002. Identity Fraud: A Study. London: Economic and Domestic Secretariat, Cabinet Office.

Cass, C. 2005. "A background briefing on Anti-money laundering.," Deloitte Touche Tohmatsu, Australia, October, pp 1-3. (Retreived March 14, 2008 from http://www.deloitte.com/dtt/alert/0,1001,cid%253D96828,00.html).

Cheney, J. S. 2005. "Identity Theft: Do definitions still matter?," Discussion paper, Payments Card Center, August, pp 1-22. Federal Reserve Bank of Philadelphia.

Choo, K-K. R., Smith, R., and McCusker, R. 2007. "Future Directions in Technology-Enabled Crime," 2007-2009, Australasian Institute of Criminology, (78), pp 1-166.

CIFAS Online. (2006). Retrieved 7 February, 2007 from http://www.cifas.org.uk/.

Conway, R.W., Maxwell, W.L., and Morgan, H.L. 1972. "On the implementation of security measures in information systems," *Communications of the ACM*, (15:4), pp 211–220.

Corbin, J. and Strauss, A. 1990. "Grounded Theory Method: Procedures, Canons and Evaluative Criteria," *Qualitative Sociology*, (13), pp 3-21.

Council of Australian Governments Agreement to a National Identity Security Strategy. 2007. "An Agreement to a National Identity Security Strategy," Australia Government, April, pp 1-9.

Council of Europe. 2004. "Organised crime situation report 2004: focus on the threat of cybercrime," Retrieved 17 February, 2007 from http://www.coe.int/T/E/Legal_Affairs/Legal_co-peration/Combating_economic_crime/8_ Organised_crime/Documents/Organised%20Crime%20Situation%20Report%202004.pdf

Crompton, M. 2004. "Proof of ID Required? Getting Identity Management Right," Australia Government, March, pp 1-33. Retrieved 18 February, 2007 from http://www.privacy.gov.au/news/speeches/sp1_04p.html.

Cuganesan, S., and Lacey, D. 2003. Identity Fraud in Australia: An evaluation of its Nature, Cost and Extent. SIRCA, Sydney.

Dhillon, G., and Backhouse, J. 2000. "Information system security management in the new millennium," *Communications of the ACM*, (43:7), pp 125–128.

Fair and Accurate Credit Trans-actions Act, 2003 Pub. Law. 108-159, 111 Stat. 1952.

Finch, E. 2003. "What a tangled web we weave: identity theft and the Internet," In Jewkes (ed.), Dot.cons: Crime, deviance, and identity on the Internet. Collompton, England: Willan, pp 86-104.

Ford, R and Charter, D. 2006."ID fraud figures 'inflated to play on public fears'". The Times, 3 February, pp 1-2.

Gordon, L., and Loeb, M. 2002. "The Economics of Information Security Investment," *ACM Transactions on Information and System Security*, (5:4), pp 438-457.

Hinde, S. 2002. "Security Surveys," *Computers & Security*, (21:4), pp 310-321.

Home Office. 2004. "New anti-ID-fraud one-stop shop," July, pp 1-2. Retrieved 3 May, 2007, from http://press.homeoffice.gov.uk/press-releases/New_Anti-Id_Fraud_One-Stop_Shop?version=1

Home Office. 2006. "United Kingdom Government," Retrieved 1 December, 2006, from http://www.homeoffice.gov.uk/.

Home Office Identity Fraud Steering Committee. 2004. "Identity Crime Definitions," United Kingdom Government, 9 December. v1.0.

Identity Theft and Assumption Deterrence Act. 1998. Pub. Law 105-318, 112 Stat. 3007 18 U.S.C.§1028.

Jamieson, R., Land, L., Stephens, G., Winchester, D. 2008. "Identity Crime: The Need for an Appropriate Government Strategy," *Forum on Public Policy Online*, Spring edition, pp 1-33.

Jamieson, R J., Stephens, G., Winchester, D W., 2007a. "An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts," Proceedings of the 11th Pacific Asia Conference on Information Systems, July 3 – 6, 2007, Auckland, New Zealand, (Paper 85) pp 1-13. Felix B Tan, James Thong, Lech J. Janczewski. (Editors), Published by the School of Business, The University of Auckland.

Jamieson, R J., Stephens, G., Winchester, D W., 2007b. "Identity Fraud: The Player Landscape in Australia," Proceedings of the 18th Australasian Conference on Information Systems, 5-7 Dec 2007, Toowoomba, Australia, pp. 770-779.

Judicial Commission of New South Wales 2008. "Sentencing Statistics, Sentencing Information System".

Karat, C., Karat, J. and Brodie, C. 2005. "Why HCI research in privacy and security is critical now. International," *Journal of Human-Computer Studies*, (63:1), pp 1-4.

Kim, R. 2007. "2007 Identity Fraud Survey Report (Consumer Version): How Consumers Can Protect Themselves," (Abbreviated Version). Javelin Strategy & Research, February, pp 1-22.

Le Lievre, E., and Jamieson, R. 2005. "An Investigation of Identity Fraud in Australian Organizations," CollECTeR LatAm 2005 Conference, Chile, pp 1-10.

Mahmood, M. A., Siponen, M., Straub, D., and Rao, H. R. 2008. "Call for Papers MISQ Special Issue on: Information Systems Security in a Digital Economy," *MIS Quarterly*, pp 1-6.

Main, G., and Robson,. B. 2001, Scoping Identity Fraud, Canberra, Commonwealth Attorney-General's Department.

McCue, A. 2006. "Government ID fraud claims - are they all they seem?," Retrieved 2 February, 2007 from http://www.silicon.com/publicsector/0,3800010403, 39156140,00.htm.

Meulen, N. 2006. "The challenge of countering identity theft: recent developments in the United States, the United Kingdom, and the European Union," 6 September, 1-36. Report commissioned by the National Infrastructure Cyber Crime program (NICC). International Victimology Institute Tilburg (INTERVICT).

Model Criminal Law Officers' Committee (MCLOC). 2008. "Final Report Identity Crime," Commonwealth of Australia, March, pp 1-46.

Model Criminal Law Officers' Committee (MCLOC). 2007. "Identity Crime," Commonwealth of Australia, Discussion Paper, Chapter 3, April, pp 1-36.

Newman, M., and McNally, M. 2005. "Identity Theft Literature Review,' Prepared for presentation and discussion at the National Institute of Justice Focus Group Meeting January 27-28, 2005, July, pp 1-114.

Office of the Privacy Commissioner of Canada. 2007. "Identity Theft – A Primer," Canadian Government, pp 1-5. Retrieved 30 March 2007 from http://www.privcom.gc.ca/id/primer_e.asp.

Porter, D. 2004. "Identity fraud: the stealth threat to UK plc," Computer Fraud & Security, July, 7, pp 4-6.

QSR NVivo. 2005. Version 2.0. QSR International Pty. Ltd, Melbourne, Australia.

Simon, J. 2008. "The credit card-terrorism connection: How terrorists use cards for everyday needs and to fund operations," CreditCards.com, May 15, pp. 1-4. Retrieved 26 September, 2008, from http://www.creditcards.com /credit-card-news/credit-cards-terrorism-1282.php.

Siponen, M., and Willison, R. 2007. "A Critical Assessment of IS Security Research between 1990-2000". In Proceedings of 15th European Conference on Information Systems, June 7-9, St. Gallen, Switzerland, pp 1551-1559.

Sproule, S., and Archer, N. 2006. "Defining Identity Theft – A Discussion Paper," McMaster University, April, pp 1-37.

Straub, D.W. 1990. "Effective IS security: an empirical study," *Information Systems Research*, (1:3), pp 255–276.

Straub, D., Goodman, S., and Baskerville, R. 2008. "Framing of Information Security Policies and Practices," In Information Security Policies, Processes, and Practices, D. Straub, S. Goodman and R. Baskerville (eds.), Armonk, NY: M. E. Sharpe.

Straub, D. W. and Welke, R. J. 1998. "Coping with Systems Risk: Security Planning Models for Management Decision-Making," *MIS Quarterly*, (22:4), pp 441-469.

Thompson, D. 1998. "Computer Crime and Security Survey," *Information Management & Computer Security*, (6:2), pp 78-101.

United States Department of Treasury. 2005. "The Use of Technology to Combat Identity Theft," February, pp 1-117. Retrieved 3 April, 2006, from http://www.treas.gov/offices/domestic-finance/financial-institution/cip/biometrics_study.pdf

Urbas, G and Choo, K. R, 2008. "Resource Materials on Technology-Enabled Crime, Technical and Background," Australasian Institute of Criminology, (28), pp 1-96.

US General Accounting Office (GAO). 2002. "Identity Theft: Prevalence and Cost Appear to Be Growing," Report to Congressional Requesters, GAO-02-363.

US General Accounting Office (GAO). 1998. "Identity Fraud: Information in Prevalence, Cost, and Internet Impact Is Limited," Briefing Report to Congressional Requesters, GAO/GGD-98-100BR.

Wang, G., Chen, H., and Atabakhsh, H. 2004. "Automatically Detecting Deceptive Criminal Identities," *Communications of the ACM*, March, (47:3), pp 71-76.

Willox, N A., Jr., and Regan, T. M. 2002. "Identity Fraud: Providing a Solution," *Journal of Economic Crime Management*, Summer, (1:1), pp 1–15.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the assistance and cooperation of participants from the organisations sponsoring this Identity Fraud Linkage Research Project and to AUSTRAC Consortium and the Australian Research Council for their research grant.

COPYRIGHT