Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodclaw.htm

Computer Law & Security Review

Addressing identity crime in crime management information systems: Definitions, classification, and empirics

Rodger Jamieson [a], *Lesley Pek Wee Land* [a], *Donald Winchester* [a], *Greg Stephens* [a], *Alex Steel* [b], *Alana Maurushat* [b], *Rick Sarre* [c]

[a] *The Australian School of Business, School of Information Systems, Technology and Management, University of New South Wales, Australia*
[b] *Faculty of Law, University of New South Wales, Australia*
[c] *School of Commerce, the University of South Australia, Australia*

Keywords:
Identity crime
Identity fraud
Identity theft
Identity deception
Computer crime
Internet
Information systems security (ISS)
Taxonomy
Personnel identifying information (PII)
Crime management information systems

ABSTRACT

Identity fraud as a term and concept in its formative stages was often presumed to be identity theft and visa versa. However, identity theft is caused by the identities (or tokens) of individuals or organisations being stolen is an enabling precursor to identity fraud. The boundaries of identity fraud and identity theft are now better defined. The absence of specific identity crime legislation could be a cause of perpetrators not classified as breaching identity crimes but under other specific entrenched law such as benefit fraud, or credit card fraud. This metrics overlap can cause bias in crime management information systems. This study uses a multi-method approach where data was collected in both a quantitative and qualitative manner. These approaches are used as a lens for defining different classes of online identity crimes in a crime management (IS) security context. In doing so, we contribute to a deeper understanding of identity crime by specifically examining its hierarchical classes and definitions; to aid clearer structure in crime management IS. We seek to answer the questions: should current law around identity fraud continue to be reinforced and measures introduced to prevent identity crime; should laws be amended; or should new identity crime laws be constructed? We conclude and recommend a solution incorporating elements of all three.

1. Introduction

The illegal online use or trade in identities of individuals and organizations is recognized to have a substantial influence on other crimes such as frauds and money laundering; seriously impacting the real economy.[1] The global economic cost of these identity crimes was estimated to be "US$2 trillion in 2005".[2] In the United States the annual estimated cost of identity crime alone in 2009 was "US$54 billion".[3] These survey figures may not reflect the actual figures if real cases were to be analysed.[4] A major concern with the costing of identity crimes is the potential bias, error, and lack of

[1] Goode, S., and Lacey, D. 2010 "Detecting Complex Account Fraud in the Enterprise: The Role of Technical and Non-Technical Controls", Decision Support Systems. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., and Sun, X. 2011. "The Application of Data Mining Techniques in Financial Fraud Detection: A Classification Framework and an Academic Review of Literature", Decision Support Systems (50:4) or (50), pp. 559–569.
[2] Hurley, J., and Veytsel, A. 2003. "Identity Theft: A $2 Trillion Criminal Industry in 2005", The Aberdeen Group 13 May, p. 1.
[3] Miceli, D., and Kim, R. 2010. "2010 Identity Fraud Survey Report: Consumer Version", Javelin Strategy & Research February, p. 5.
[4] For example, the Uniform Crime Reports have different statistics than the National Crime Victimisation Surveys in the US. See Chen, H., Schroeder, J., Hauck, R. V., Ridgeway, L., Atabakhsh, H., Gupta, H., Boarman, C., Rasmussen, K., and Clements, A. W. (2002). "COPLINK Connect: Information and Knowledge management for Law Enforcement", Decision Support Systems (34), pp. 271–285.

0267-3649/$ – see front matter © 2012 Rodger Jamieson, Lesley Pek Wee Land, Donald Winchester, Alex Steel, Alana Maurushat, Greg Stephens, and Rick Sarre. Published by Elsevier Ltd. All rights reserved.
doi:10.1016/j.clsr.2012.03.013

consistency in how they are defined and classified.[5] As crime management information systems (IS) transition from paper-based to digital systems to ease storage and aid retrieval (often remotely for law enforcement), there is an emergent need to classify the fields accurately.[6]

The US leads the way in criminalizing identity crime and data breaches.[7] (IS) security research focuses on computer abuse, computer crime, and computer-related crimes. Computer crimes include "crimes whereby the computer is the target or the mechanism for committing the crime or the computer user is the target. It also includes crimes committed over the Internet or where the Internet plays a role in the commission of the crime" (see Table 6).[8] Online identity crimes are linked to computer abuse, computer crime and computer-related crime in IS security, because they are enabled by computers and/or the Internet. A difference is that identity crime involves social engineering of people and technology.

The ubiquity of information technology; computers, the Internet, mobile devices, and their interconnectedness in a digital economy enables the increase of identity crime methods, such as phishing, not previously accounted for by computer crime and abuse in IS research.[9] Internet users reached the 2 billion mark in January 2011.[10] Smart perpetrators are devising increasingly sophisticated ways of committing identity crimes. Therefore classes of IS-enabled abuse, such as identity crime, continue to evolve often ahead of IS security innovations.[11]

The remainder of this paper is structured as follows. The next section discusses the methodology.[12] Then we identify the various definitions of identity crime and discuss our results. The final sections discuss the contributions, implications, limitations, conclusion and future research in this area.

2. Methodology

We use a multi-method research design consisting of qualitative methods and quantitative methods via secondary data to investigate how identity crime terms are defined and how the categories shape organizational actions for measuring and improving IS security to reduce identity crimes.[13] We collected qualitative data from Australia via 10 face-to-face interviews and two by teleconference in 2002. In 2002 Australia had no legislation that specifically targeted identity crime and this was a unique out-of-sample setting to study identity crimes as other jurisdictions such as the United States had enacted identity crime legislation. We also gathered data from communications with Attorney Generals and Crime Collection agencies until 2010 from many countries. All qualitative data has been continuously updated from secondary sources. From our interview transcripts, we derived themes using NVivo qualitative software.[14] The data was collected from Attorney General's departments and Government Statistics Agencies from Australia (Federal and States), Canada, European Union, Ireland, Netherland, United Nations, United Kingdom, and the US (Federal and States). The data was based on questions of identity crime definitions and their crime classification systems in use. We also obtained conditional access to the ABS Personal Fraud data collection to reclassify their identity crime data[15] for our empirical quantitative identity crime data testing, using our definitions and classification.

Interviewees were drawn from diverse industries such as banks, retailers, telecommunications, utilities, State Government licensing authorities, Federal Government agencies (welfare, immigration), and a US academic/criminologist for insights from the US. The organizations selected for interviewing represented those most targeted by identity crime perpetrators. Their credibility can be attested by the senior positions they held for instance in fraud, fraud management, compliance, and/or internal auditing. Some of the interviewees were previously employed in law enforcement or the legal profession. The interview instrument contained mainly 13 questions. Each interview lasted approximately one and a half hours. Interviewee recordings were professionally transcribed, checked for reliability and accuracy, and corroborated by members of the research team. The rich data and information gathered via email correspondence and/or telephone

[5] Romanosky, S., Telang, R., and Acquisti, A. 2008. "Do Data Breach Disclosure Laws Reduce Identity Theft?", Carnegie Mellon University pp. 1–30.

[6] Chen, above note 4. See also Orlikowski, W. J., and Iacono, C. S. 2001. "Research Commentary: Desperately Seeking the "IT" in IT Research – A Call to Theorizing in the IT Artifact", Information Systems Research (12:2), pp. 121–134, and Sproule, S., and Archer, N. 2007. "Defining Identity Theft", IEEE Computer Society, Eighth World Congress on the Management of eBusiness pp. 1–11.

[7] Romanosky, above note 5. See also Maurushat, A., "Data Breach Notification Law Across the World from California to Australia" Privacy Law and Business International, April, 2009.

[8] Douglas, J. E., Burgess, A. W., Burgess, A. G., and Ressler, R. K. (Eds. 2nd edition). 2006. Crime Classification Manual, San Francisco, CA, Jossey-Bass. Parker, D. B. 1976. Crime by Computer. New York, Charles Scribner's Sons.

[9] Bryant, R. (Ed.) 2008. Investigating Digital Crime. England, John Wiley & Sons Ltd.

[10] Statement of ITU Secretary General, Dr. Hamadoun Toure, January 26, 2011 available at http://www.who.int/topics/millennium_development_goals/accountability_commission/ITU_SG_statement_26Jan2011.pdf.

[11] Biegelman, M. T. (ed.) 2009. Identity Theft Handbook: Detection, Prevention, and Security. John Wiley & Sons, Inc. *See also* Berg, S. 2008. "Preventing Identity Theft Through Information Technology", in Perspectives on Identity Theft, M. M. McNally, and G. R. Newman (Eds.), Crime Prevention Studies, (23), pp. 151–167. Monsey, NY, U.S.A., Criminal Justice Press.

[12] McKelvey, B. 1982. Organizational Systematics: Taxonomy, Evolution, Classification. Berkeley, CA. University of California Press. *See also* Stuessy, T. F. (2nd edition) 2009. Plant Taxonomy: The Systematic Evaluation of Comparative Data. New York, Columbia University Press.

[13] Ashakkori, A., and Teddlie, C. 1998. Mixed Methodology: Combining Qualitative and Quantitative Approaches. Thousand Oaks, CA, Sage Publications. Corbin, J., and Strauss, A. 1990. "Grounded Theory Research: Procedures, Canons, and Evaluative Criteria", *Qualitative Sociology* (13:1), pp. 3–21. Glaser, B. G., and Strauss, A. L. 1967. The Discovery of Grounded Theory. Chicago: Aldine.

[14] QSR NVivo. 2008. Version 2.0. Melbourne, Australia, QSR International Pty. Ltd.

[15] Australian Bureau of Statistics. 2008a. 4528.0 Personal Fraud 2007. Australian Bureau of Statistics, June, pp. 1–40.

Table 1 – Proposed identity crime definitions.

Identity crime is a generic term that covers identity fraud, identity theft, and identity deception acts or events. It also applies to identity crime related crimes such as terrorism, money laundering, and trafficking (people, drugs, weapons, illicit material) enabled by identity fraud, identity theft, and identity deception where the purpose of the perpetrator is to seek anonymity, avoid detection, or shift the blame.

Identity fraud is the deliberate use (in criminal law terminology the combination of a physical act element and a mental fault element of intention, knowledge or recklessness) of identity theft and/or identity deception details (documentation or personal identifying information) for a financial gain, avoidance of a loss, or to seek anonymity to commit identity-related crimes (money laundering, trafficking, or terrorism acts).

Identity theft is the unlawful obtaining of identity documentation details (including personal identifying information used in customer not present situations or when customers interface with machines to authenticate, for instance personal identification numbers (PINs), passwords, key tokens, or biometrics).

Identity deception is misrepresentation through:

i. Creation of a false identity or changes to an existing identity through alteration of existing data, or the context of the data, relating to the identification of a real individual or entity, such as via a change of name, change of initials, change of residency details, change of date of birth etc.
ii. Creation of a false identity based on fake (i.e. fictitious) identification data
iii. Creation of false identification documentation both novel and counterfeit.

Source: Extended from Jamieson et al. (2008).

communications with government Attorney Generals and Statistic agencies were similarly analysed for main themes. Secondary data collected on the relevant literature by key word searches of library, Internet, legislation and other proprietary databases using terms such as, identity crime, identity fraud, identity theft, and identity deception or synonyms. Data obtained from secondary sources, enabled the discovery of more detailed and refined concepts.

3. Identity crimes

The major objective for this paper is to refine identity definitions and improve identity crime classes reducing class overlap or ambiguity. Identity crime involves the illegal use of any part of a biometric, attributed or biographical identity of an individual and entity.[16] These three identity components are used by governments and organizations to identify and authenticate customers in everyday business transactions. The identity crime label is an overarching class that encompasses identity fraud. Identity fraud is enabled by identity crime sub-classes identity theft and identity deception. The following Tables define and refine existing identity definitions. Fig. 1

Confusion between the labels – identity theft and identity fraud – was due to the evolving nature of the definitions within different countries (see Table 6). Second, within the sub-class 'identity deception', numerous other labels are often used, for example identity falsification, identity fabrication, fake identity, false identity, or synthetic identity. Similarly, within the 'identity theft' sub-class other names in use may include identity appropriation, and true name identity. The variety of terminology and the dynamic nature of identity crimes' sub-classes exacerbate definitional and classificatory uncertainty.

In the development of identity crime legislation and its judicial interpretation, legal authorities would be assisted by a shared vocabulary and classification of crime types. While the full range of identity-related crimes is too broad and evolving to be able to precisely or usefully define in legislation, significant clarity can be achieved in definition of sub-categories of identity crime. Reaching a consensus among stakeholders for the meaning of identity crime terms also has major implications in data and information collection, analysis, and dissemination of outputs across time and locations for comparison.[17]

As a result of ambiguous crime class definitions and the lack of crime theories used in IS research, the metrics used to record trends in newer computer-related crime facilitated abuse methods like identity crime are not consistently collated or comparable.[18] Hence specific information about these crimes is not easily retrievable.[19] This is a critical research gap when determining the theory for explaining computer and online identity crime situations.[20] Recently, there is support in an IS security context to investigate identity theft, Cybercrime, electronic fraud, credit card fraud, anti-phishing and privacy methods by applying criminological theories.[21] Proper classifications will enable a better understanding of the relative level of this identity crime activity and

[16] Kim, R. 2008. "2008 Identity Fraud Survey Report Consumer Version: How Consumers Can Protect Themselves", Javelin Strategy & Research pp. 1–23.

[17] Model Criminal Law Officers' Committee. 2008. Final Report Identity Crime. Commonwealth of Australia, March, 1–46.

[18] Goode, above note 1.

[19] OECD. 2008. Scoping Paper on Online Identity Theft. Organisation for Economic Co-operation and Development, DSTI/CP(2007)3/FINAL, January, pp. 1–69.

[20] Liang, H., and Xue, Y. 2009. "Avoidance of Information Technology Threats: A Theoretical Perspective", MIS Quarterly (33:1), pp. 71–90. *See also* Berg, above note 12; and Orlikowski, above note 6.

[21] Mahmood, M. A., Siponen, M., Straub, D., and Rao, H. R. 2008. "Special Issue – Call for Papers – Information Systems Security in a Digital Economy", *MIS Quarterly* pp. 1–6. Smith, S., Winchester, D., Bunker, D., Jamieson, R. 2010. A Study of Mandated Compliance to an Information Systems Security de jure Standard in a Government Organization. MIS Quarterly (34), 463–486.

its impact on organizations and individuals, in making generalizations over time nationally and internationally.[22] This process is complicated when there may be more than one (legal) jurisdiction within a country, as in Australia, Canada or the US, among others.

The main purpose of crime metrics in management IS gathered by national statistics collecting bodies or at the law enforcement case level is to have a history of relationships that could help authorities to understand and develop countermeasures for crimes.[23] However, these relationships are often unclear or imprecise, due to method biases. This is in part due to perpetrator acts not given proper definitions to determine classification boundaries.[24] In fact, in some instances in the US and Australia, State statistic collecting bodies have more granular data collection categories than a Federal agency and they must periodically align their more granular crime data via conversion tables.[25] In other cases, if only aggregated data is kept, then the advantages of precision in collections are lost by merging data with another less granular crime data class potentially subverting the original data collection purpose(s) of the IS. The similarities between identity crimes, computer crime, and fraud in general, give us a clue as to where we can start to refine identity crime definitions and classifications, and to observe linkages, or find overlaps, whether by homogeneity or heterogeneity, between classes.

4. Discussion of results

Identity theft and identity deception are also enablers of identity fraud as well as other related economic crimes such as money laundering, terrorist financing, drug trafficking and people smuggling.[26] In Australia, people committing identity crimes may be prosecuted under current legislation such as bank fraud, credit card fraud, or mail fraud (see Table 5), or under some other legislation where specific identity crime laws are absent such as in certain Australian States. Herein lies a dilemma for government, law enforcement, practitioners, and academic researchers[27]; should current law continue to be reinforced, laws be amended, or new identity crime laws be constructed? Based on our findings in this study, we promote a combination of these options. We now outline our reasons.

The evolution of identity crimes such as identity theft had its beginnings well before 1964 when the term 'identity theft' was first documented. Similar crimes were well known to US law enforcement agencies in postal services and the credit card industry.[28] These criminal behaviours of committing fraud were perpetrated by stealing credit cards from the mail from the 1960s. Mail theft itself was a problem in the US from the start of the US Postal Service in 1775. United States legislation was subsequently passed in the late 18th century to criminalize mail theft.[29] Similarly, 'wire fraud' was and continues to be a problem in the US and other jurisdictions as communications technology evolves from fixed line to mobile telephony and the Internet or a hybrid system (for example Voice over Internet Protocol). Some forms of conduct have been criminalized, as policy-makers (often due to public pressure) have sought to use the legal system to establish or to reinforce acceptable social norms, culture, and attitudes.

A reasonable starting point to assess the general evolution of crime leading to identity crime sub-classes is to investigate the norms or attitudes that may have influenced the cultures in countries that currently have identity crime laws (Australia, Canada, US). Thus, crime classification systems vary by jurisdiction although there are some commonalities. Major crime categories (for example, murder, fraud, or theft) and their heuristics also determine how sub-classes of these crimes have evolved. The evolutionary changes in fraud in Australia have been documented and changes may differ when compared with other countries.[30] Fraud, while not being a new crime, is a crime that is in a state of change and evolution due to shifting IS technologies.[31] As the scope of the identity crime problem (in both economic and societal terms) increases, similar pressures have been placed on government policy makers to legislate against it.[32] The use of identity deception techniques for committing crimes is not a recent phenomenon. For example, the English Forgery Act was passed in 1870 to legislate against false share certificates. The evolution of specific identity crime taxonomy via a classification (process) correlates closely with the introduction of legislation firstly in the US and subsequently in Australia or

[22] Sproule, S., and Archer, N. 2008. "Measuring Identity Theft in Canada: 2008 Consumer Survey", McMaster eBusiness Research Centre (MeRC) DeGroote School of Business (23), pp. 1–70. Foley, L., Barney, K., and Foley, J. 2010. "Identity Theft: The Aftermath 2009", Identity Theft Resource Center, pp. 1–45. Halperin, R., and Backhouse, J. 2008. "A Roadmap for Research on Identity in the Information Society", Identity in the Information Society Journal (1:1), pp. 1–17. Parsons, J., and Wand, Y. 2008. "Using Cognitive Principles to Guide Classification in Information Systems Modeling", MIS Quarterly (32:4), pp. 839–868. US General Accounting Office. 2002. Identity Theft: Greater Awareness and Use of Existing Data are Needed. June, pp. 1–72. See also OECD, note 20.

[23] Kraus, L. I., and MacGahan, A. 1979. Computer Fraud and Countermeasures. Englewood Cliffs, New Jersey, Prentice-Hall, Inc. See also Mahmood, note 21.

[24] Warner, S. B. 1931. "Crimes Known to the Police: An Index of Crime?", Harvard Business Review (45:2), pp. 307–331.

[25] Australian Bureau of Statistics. 2008b. *Australian* Standard Offence Classification (ASOC) 1234.0, (2nd Ed.), Australian Bureau of Statistics, August, pp. 1–172. Castle, C., and Sampson, L. 2008. JANCO Classification System. Government of South Australia – Office of Crime Statistics and Research, May, pp. 1–41.

[26] Chen, above note 4. Wang, G., Chen, H., and Atabakhsh, H. 2004. "Automatically Detecting Deceptive Criminal Identities", Communications of the ACM (47:3), pp. 71–76.

[27] Gill, G., and Bhattacherjee, A. 2009. "Whom are we Informing? Issues and Recommendations for MIS Research from an Informing Sciences Perspective", MIS Quarterly (33:2), pp. 217–235.

[28] Straub, D. 1989. "Validating Instruments in MIS Research", MIS Quarterly (13:2), pp. 147–169.

[29] Biegelman, above note 11.

[30] Goode, above note 1.

[31] Goode, above note 1. *See also* US Government. 2007. Combating IDENTITY THEFT: A Strategic Plan. The President's Identity Theft Task Force, April, pp. i-110.

[32] Stephan, M., Pennington, S., Krishnamurthi, G., and Reidy, J. 2009. Identity Burglary. Texas Review of Law and Politics (13:1), pp. 401–418. Stevenson, C. L. 1944. Ethics and Language. New Haven, Connecticut, Yale University Press.

Table 2 – Hierarchically ordered identity crimes sub-classes.[a]

Identity act or event name	Classification	Context	Region	Reference
Identity crime	Top category	Tax Crime	Australia	Australian Tax Office (2009)
Identity fraud	Category			
Identity creation	Category			
Identity theft/takeover	Sub-category			
Database identity (Population),	Category	Legislation,	Australia, UK	Sullivan (2009)
Token identity (Individual)	Sub-category			
Identity crime	Category	Legislation, maintaining the integrity of the nation's (US) financial infrastructure and payment systems	US, International	US Secret Service (2010, http://www.secret service.gov/criminal.shtml)
Credit card/access Device fraud (Skimming),	Sub-category			
Identity theft,	Sub-category			
False identification	Sub-category			
Passport fraud,	Sub-category			
Bank/check fraud	Sub-category			
Identity (Theft) appropriation	Category	Identity crime legislation	Australia	Model Criminal Law Officers' Committee (2008)
Identity fraud	Category	Extent and nature survey	Canada	Sproule and Archer (2008; 2007)
Identity theft	Sub-category			
ID-related crime	Category	Conceptual, Technical, legal	UK	Koops et al. (2009)
Identity deletion	Sub-category			
ID-related crime	Umbrella term	Policy, Research	UK	Koops and Leenes (2006)
Identity fraud	Category			
Identity theft	Sub-category			
Identity crime	Top category	Policy, research, meaningful data collection, analysis and comparisons across jurisdictions	Australia, New Zealand, Asia-Pacific	Jamieson et al. (2008)
Identity fraud	Category			
Identity theft	Sub-category			
Identity deception	Sub-category			
Identity-related crime	Category			
Identity collision	Category	Policy, research	UK	Leenes (2006b, ed.) Rost, Meints, and Hansen (2006)
Identity change	Category			
Identity takeover	Sub-category			
Identity exchange	Sub-category			
Identity delegation	Sub-category			
Identity creation	Sub-category			
Identity deletion	Category			
Identity restoration	Category			
Identity[b]	Category	Information society (A set of concepts)	UK, EU	Anrig et al., 2005
Subjects	Sub-category			
Virtual persons	Sub-category			
Identity crime	Top Category	Policy, Research	Australia	Australasian Centre for Policing Research 2006
Identity fraud	Category			
Identity theft	Sub-category			
Identity theft	Category		US	Cheney 2005

a Legislation makes an act or event a crime.
b Identity: identification, anonymity, pseudonymity, (un)observability, (un)traceability.

Canada, with other countries beginning to follow, for example the UK. The basis of taxonomy is evolutionary connectedness.

Identity crimes are a problem directly associated with identity attribution and system authentication such as a credit card PIN or username and password. Identity crime is not an industry specific crime. Identity crime permeates across all sectors and countries where personal and organizational identity information is used for economic gain or avoidance of cost or loss. The grouping and ranking in hierarchies, by similarities or differences between identity crime classes are shown in Table 2.

Reading Table 2, we see the many different identity crime nomenclature, classifications by rank, context, and jurisdictional region; these identifications by the individuals gave referral to their taxon referenced by author(s). Table 2 column 1, shows a vast array of identity crime nomenclature used across and within regions as well as their evolving classification labels.

Both identity theft and identity deception have many crime sub-class methods at the most granular level. Well-known examples of offline identity theft are caused by wallet theft, mail redirection, and dumpster diving, while an example of an online identity theft method is war-driving. Online examples for identity deception are phishing, vishing, and smishing.[33]

[33] Urban, M. 2006. "The Evolution of Phishing", ISSA Journal September, pp. 1–53.

Table 3 – Participant interviewees insights on the meaning of identity crime.

Participant	Selected interviewee insights on the meaning of identity crimes
	Australian private organizations
1	"We have no document (in Australia) that was originally designed and/or issued with all the necessary checks, balances data matching and enquiries to prove someone's identity. If we can get that process right then you can start building the process, working up from that and that is where it simply falls over."
2.1	"if identity crime was easy to describe we probably wouldn't be sitting here because there would have been a measure around it. I mean that's the problem."
3.2	"In terms of what we've got to get down to is defining exactly what identity theft or identity fraud is. What it requires is the actual adoption or use of someone else's identity in order to commit that fraud. Where banks mainly see identity fraud is in the false applications for things like credit cards and so forth."
3.1	"I think there's some use in defining or distinguishing between identity theft and identity takeover (identity deception), in that we categorize frauds where a person has been in fact made up, if you like fictitious, using false identification documentation. We categorize that differently to takeover of a legitimate person's identity. It is somewhat easier to perpetrate a takeover and obviously there is social engineering involved. "I think it is worthwhile to note that historically the bank has classified identity fraud, based on product or service delivery channel. We've classified that as by the product it's been paid for."
6	"Identity fraud for me indicates that the identity that's been presented is false, like counterfeit or something like that. We get a lot of true name fraud, but it's usually new accounts. They are not usually existing customers or added onto an existing customer account. It is usually dealers."
	Australian Government – federal and state agencies
4	"From an external fraud point of view, [what] we try to address are; illegitimately issued and fraudulently obtained State photo driver licenses; Motor vehicle re-birthing associated with fraudulent identities; fake State driver licenses used as proof of identity in commercial frauds; fraudulently obtained, misused, or manufactured Proof of Age cards; gun and security licenses and associated impact on the integrity of the XXX Transport Authority's policies/procedures and records; and fraudulently obtained, misused or manufactured mobility parking system authorities."
7	"We define identity fraud as relating to the actual, the physical person, and their name."
8	"We have a definition for identity fraud where it is "the misuse of an identity to claim, to receive government payments in excess of the general entitlement. We certainly sub-define it down to different levels of fictitious identity, created identity, assumed identity. Accordingly, each one of those would be approached in a different way because they manifest themselves differently. Each type of category requires a different approach."
9	"identity fraud under two broad categories; assumed identity (identity deception) and stolen identity (identity theft)".
10	The big area where there are issues, is in account opening identification, is of course fake or stolen documents. That's actually prohibited by legislation."[a]
11	"We say identity fraud is basically someone saying who they are not. They pretend to be someone else".
	US Academic
12	"Earlier on when the identity crime literature started to develop people were referring to it as identity theft. That has now migrated to a new term, identity fraud, because identity frauds are a larger category. There is a need to create some type of typology of identity frauds because there are new forms emerging all the time and maybe more than one typology would be better. For a while there were no statutes governing or very loose statutes governing identity crimes (such as identity theft or identity fraud) those statutes have tightened up so now. What makes anything a crime is a statute."

a The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) received Royal Assent on 12 December 2006. In the US a similar law is; Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001.

Identity deception is a broader cause of criminality than identity theft because stealing an identity is just one of many classes of identity crime that allows someone to assume an identity of another individual or entity (real or fictitious). The identity deception class has been recommended to be further classified into sub-classes identity manipulation and identity falsification and each has been given similar labels.[34] The Australasian Centre for Policing Research (2006) and Model Crime Law Officer's Committee (2008) identity crime definition also includes the situation for when someone creates a false identity that is not based on a real person; a fictitious identity. We label this identity deception. Identity crime generally means activity in which a perpetrator utilizes a false identity in order to facilitate the commission of a crime; with nomenclature labelled identity fraud or sub-classes ranked identity theft and identity deception categories.

Interview quotes from Participant 12 in Table 3 illustrate the need for and problems around, the requirement to initially define a new phenomenon such as identity fraud and identity theft or to classify the many other labels for identity deception. Until the terms are defined within statutes and improved upon with amendment(s) and/or case law, law enforcement case charges are usually laid against an identity crime (or any

[34] Australasian Centre for Policing Research. 2006. "Standardisation of Definitions of Identity Crime Terms: A Step Towards Consistency", Report Series, (145.3), March, pp. 1–17. United Kingdom Home Office Identity Fraud Steering Committee. 2004. Identity Crime Definitions. 9 December. v1.0. *Also see* Table 3 interviewee 3.1 quotes for example.

Table 4 – Selected examples of participant feedback from email correspondence with US experts within a specific jurisdiction.

US State	Correspondence feedback
California	"Although the California Penal Code does differentiate crime against property from other crimes, identity theft is not one of the crimes that are required to be tracked in California. One of the major challenges in tracking identity theft crimes in California is that an identity theft crime may be charged as a number of different crimes. For example, an identity theft case that involves stalking may resolve as stalking."
Delaware	"The (identity theft) law was enacted in 2000 as a class E felony but was changed to the more serious Class D felony in 2004".
Idaho	"Idaho state law pertaining to identity theft is codified under Title 18 of the Idaho Code, Chapter 31 ("false pretenses, cheats, and misrepresentations"), [see http://www.legislature.idaho.gov/idstat/Title18/T18CH31.htm]. Section 18–3126 relates specifically to identity theft".
Indiana	"I work in the Attorney General's Identity Theft Unit, and we worked with our legislature to pass an identity theft bill earlier this year. Our identity deception (and new synthetic identity deception) statutes can be found at http://www.in.gov/legislative/ic/code/title35/ar43/ch5.html. Other criminal offences are contained in Title 35 of the Indiana Code (see http://www.in.gov/legislative/ic/code/title35/)".
Montana	"Theft is a "top-level" classification. I'm sure you have heard the expression "index crimes". According to the index, MN statutes (and therefore offences) on identity theft are categorized under 'theft'. However, the Montana Incident-Based Reporting System (MTIBRS) (Montana's crime data collection system), identity theft is classified as a fraud. But depending on the incident, any number of offences could be included with the identity theft, such as writing a bad check, credit card theft/unlawful use of a credit card, or embezzlement. Montana does not use any sub-classification in any data collection efforts. In MT's crime incident reporting handbook, we have a number of indexes that show the relationship between Montana's MCA/MTIBRS codes and how they relate to the FBI's codes. Lastly, you would be correct by saying that our "fraud" category would be inflated by including identity theft".
North Carolina	"The law gets divided into criminal or civil law. So depending on the severity and nature of the act, identity theft could be a crime or a civil issue. Most of the identity crimes are handled on the local level, not the state level. We spend most of our time educating citizens on how to protect themselves".
North Dakota	"We do not have statistics relating to identity theft because it is not, generally, prosecuted as a criminal offense and because reports can be filed with local law enforcement OR with this office (AG's) OR with the Federal Trade Commission. There is no requirement for reporting among agencies".
New Mexico	"The Attorney General's Office is now required by law to collect statistics on identity theft (passed this year). As they have just started this collection process they do not have any figures currently available. Statistics on identity theft in the US are fairly non-existent. Here is an excerpt from the US Department of Justice Website: In contrast to Federal Trade Commission extensive database of consumer complaints and victimization, the criminal justice system lacks any such information related to identity theft. No criminal justice agency maintains a national database of the number of identity theft cases".
Nevada	"In Nevada by various statutes, crimes are classified as Category A, B, C, D, and E felonies, Gross Misdemeanors, and Misdemeanors".
Ohio	"Ohio is a Home Rule State and with that we do not have any one entity that governs the other when it relates to identity crimes. Law enforcement would be the entity that would investigate any of the white collar crimes such as identity theft, economic, cyber, computer, or organized crime, theft and fraud".
Oregon	"Identity theft is one of those offences that tend to get lost among other offences because of the grouping we have to do. In Oregon we have 2 crime reporting formats. Law enforcement agencies reporting in our older format (about 68%) report identity theft as 'Fraud-By Deception'. The remaining 32% of the law enforcement agencies in Oregon who use our newer reporting format (called O-NIBRS) report identity theft as 'Fraud-Impersonation'".
Tennessee	"Identity theft is generally categorized as an economic crime though it begins quite often as simple theft."

other 'new' crime for that matter) perpetrator under a current statute, for example, mail fraud, telephone fraud, credit card fraud, or check fraud. There is a need to define identity crimes in legislation because 'identity theft' and 'identity deception' are enablers of 'identity fraud'. There is a range of crimes then which impact communities in devastating ways.[35] All these intricacies in identity crime terms we clearly define in Table 1 grounded from interviewee data collection; this is the level at which identity crime definitions need to be considered for accurate research and comparison of results across time and location.[36] We attained these definitions upon considering themes from coded data.

Participant 8 alludes to perpetrators using fictitious identities, which can manifest itself in different ways. With fictitious identity, perpetrators may eventually exist within organizational knowledge management systems. Organizations or government can find it difficult to discover false identities within their databases, or in via other interactions in the community. This is because identity fraud perpetrators can create an identity by registering on other databases, or with other organizations through exploiting weak attribute checks or authentication systems. Perpetrators might for instance register on the electoral roll, create bank accounts or to obtain a driver's license if the authenticity checks of any of these systems can be circumvented. If successful, perpetrators have then created an identity which is likely to be able to authenticate further uses in other databases, because organizations are unlikely to look behind

[35] Chua, C. E. H., Wareham, J., and Robey, D. 2007. "The Role of Online Trading Communities in Managing Internet Auction Fraud", *MIS Quarterly* (31:4), pp. 759–781.
[36] Corbin, above note 13.

Table 5 – Identity crime legislation.

Country/Level	Legislation	Effective	Description (Abridged)
Australia[a] *Federal Level (Commonwealth and the Territories):*	*Criminal Code Act 1995*, Schedule ('The Criminal Code') Part 10.8—Financial information offences	31 August 2004	These provisions prohibit dishonestly obtaining, or dealing in, "personal financial information"[b] without the consent of the person to whom the information relates; or possessing, controlling or importing any "thing" with the intention that the thing be used to commit the offence of dishonestly obtaining or dealing in personal financial information. These offences are primarily directed at: "credit card skimming" and "phishing" but may have a broader reach.
	Criminal Code Act 1995, Schedule ('The Criminal Code') Part 9.5—Identity crime	3 March 2011	Under these provisions a person (the first person) commits an offence if: (a) the first person deals in identification information; and (b) the first person intends that any person (the user) (whether or not the first person) will use the identification information to pretend to be, or to pass the user off as, another person (whether living, dead, real or fictitious) for the purpose of: (i) committing an offence; or (ii) facilitating the commission of an offence; and (c) the offence referred to in (b) is an indictable offence against a law of the Commonwealth
State Level: South Australia	*Criminal Law Consolidation Act 1935* Part 5A—Identity Theft	5 September 2004	These provisions make it an offence for a person to assume a false identity, or falsely pretend to have particular qualifications or a particular capacity, intending, by doing so, to commit, or facilitate the commission of, a serious criminal offence. It is also an offence to use another person's personal identification information to commit, or facilitate the commission of, a serious criminal offence.
Queensland	*Criminal Code Act 1899*s 408D—Obtaining or dealing with identification information	7 February 2007	Under these provisions, it is a 'misdemeanour' for a person to obtain or deal with another entity's identification information for the purpose of committing, or facilitating the commission of, an indictable offence. It is also an offence to possess equipment for the purpose of committing, or facilitating the commission of, the aforementioned misdemeanour.
Western Australia	*Criminal Code Act Compilation Act 1913*, Appendix B (*Criminal Code Act 1913*) Schedule (The Criminal Code) Division III Chapter LI—Identity crime	Assented 25 June 2010 (Criminal Code Amendment (Identity Crime) Bill 2009), not yet commenced	Upon commencement of these provisions, it would be an offence for a person to make, use, possess or supply identification material with the intention that the material will be used, by the person or some other person, to commit, or facilitate the commission of, an indictable offence.
Victoria	*Crimes Act 1958* Part 1 Division 2AA—Identity crime	17 June 2009	It is an offence for a person to make, use, possess or supply identification information (not relating to that person), if the person is aware that the information is identification information (or is aware that there is a substantial risk that the information is identification information), and intends to use or supply the information to commit, or facilitate the commission of, an indictable offence.
New South Wales	*Crimes Act 1900* Part 4AB—Identity offences	12 November 2009	It is an offence for a person to possess or deal in identification information with the intention of committing, or facilitating the commission of, an indictable offence. It is also an offence for a person to possess any equipment, material or other thing to make identification documents or other things with the intention to use these documents or things to commit, or facilitate the commission of, an indictable offence.

Table 5 – (*continued*)

Country/Level	Legislation	Effective	Description (Abridged)
Canada *National Level:*	Criminal Code (RSC, 1985, c C-46) Sections 402.2, 403	22 October 2009 (S-4 *An Act to Amend the Criminal Code (Identity Theft and Related Misconduct)*)	It is an offence for a person to knowingly obtain or possess another person's identity information in circumstances giving rise to a reasonable inference that the information is intended to be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence. It is an offence for a person to transmit, make available, distribute, sell or offer for sale another person's identity information, or have it in their possession for any of those purposes, knowing that or being reckless as to whether the information will be used to commit an indictable offence that includes fraud, deceit or falsehood as an element of the offence. It is an offence for a person to fraudulently personate another person, living or dead, with the intent: to gain advantage for themselves or another person; or to obtain property; or to cause disadvantage to the person being personated or another person; or to avoid arrest or prosecution; or to obstruct, pervert or defeat the course of justice.
Norway *National Level:*	The Penal Code	2009	It is an offence to, without authority, possesses of a means of identity of another, or to act with the identity of another or with an identity that easily may be confused with the identity of another person, and with the intent of a) procuring an economic benefit for oneself or for another person, or b) causing a loss of property or inconvenience to another person."
United States *Federal Level:*	False Identification Crime Control Act of 1982, Pub L No 97-398, 96 Stat. 2009; 18 USC § 1028	31 December 1982	Under certain circumstances, it is an offence for a person to knowingly and without lawful authority produce an identification document, authentication feature, or a false identification document ('ID documents'); to transfer ID documents knowing that they are stolen or produced without lawful authority; to possess ID documents with the intention that they be used to defraud the United States; to produce, transfer or possess a document-making implement or authentication feature with the intention such document-making implement or authentication feature will be used in the production of a false identification document; or to knowingly traffic in false or actual authentication features for use in false identification documents, document-making implements, or means of identification. It is also an offence for a person to knowingly transfer, possess, or use, without lawful authority, a means of identification of another person with the intent to commit, or to aid or abet, or in connection with, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.
	Internet False Identification Act of 2000, Pub L No 106-578, 114 Stat 3075; 18 USC § 1028	28 December 2000	These provisions cover computer-facilitated crimes of false identity and prohibit the possession, production, or transfer of false identification documents or identification documents that were not legally issued to the possessor. They also prohibit the production, transfer, or possession of any "document making implement" that is intended for use in manufacturing false identification documents.
	Identity Theft and Assumption Deterrence Act of 1998 Pub L No 105–318, 112 Stat 3007; 18 USC § 1028A	30 October 1998	Under these provisions, it is an offence for a person, during and in relation to certain listed felonies, to knowingly transfer, possess, or use, without lawful authority, a means of identification of another person or a false identification document.

(*continued on next page*)

Table 5 – (*continued*)

Country/Level	Legislation	Effective	Description (Abridged)
	Identity Theft Penalty Enhancement Act, as amended by Pub L No 108-275, 118 Stat 831; 18 USC § 1028A	15 July 2004	The Identity Theft Penalty Enhancement Act amends the US Code to establish penalties for aggravated identity theft in addition to the existing punishments for related felonies. The act adds 2 years to prison sentences for "knowingly transferring, possessing, or using, without lawful authority, a means of identification of another person" and 5 years for false identification in the commission of "terrorist acts."
State Level:	All US States have some form of identity crime (labelled identity theft, identity fraud, or identity deception) legislation	Beginning with Arizona in 1996	Crime offence reports can be filed with local law enforcement or at a state Attorney General's office (for example, under North Dakota consumer fraud division) or with the Federal Trade Commission. There is no requirement for reporting among agencies. Each State has their own rules on legislation matters. Most state agencies use the Uniform Crime Reporting Manual for reporting crime statistics which is published by the Federal Bureau of Investigation.

a For a detailed critical analysis of all Australian identity crime offences see Steel, A. "The True Identity Of Australian Identity Theft Offences: A Measured Response Or An Unjustified Status Offence?" 33 (2010) University of New South Wales Law Journal 503–531.
b "Personal financial information" is, for constitutional reasons, defined as information relating to a person that may be used to access funds, credit or other financial benefits, where those funds are deposited with, or the credit is offered by, a corporation or an authorized deposit-taking institution within the meaning of Banking Act 1959. Practically speaking, this will cover almost all financial institutions.

these apparently genuine documents.[37] Alternatively, a perpetrator could also create another identity under a different name by simply transposing letters or by dropping a letter in a first or last name. Similar instances have occurred by mistakes in administration, for example a clerk might make a spelling or typing error on an identity document and this allows a perpetrator to opportunistically represent that altered name as their own. Assumed identities emerge also, where one can either take on the identity of a living person, a genuine person, or a dead person. Therefore systems need resilience to be able to absorb and recover from such perpetrator attacks.[37] A recent Australian innovation is for organizations to set up processes to trawl through 'fact of death' files to determine identities on their databases are deceased.

Private organizations see identity fraud, identity theft and identity deception (or synonyms) in a much narrower nomenclature than government agencies. While Australian Federal and State agencies in some cases adopt their own internal group labelling for the various identity crime subclass names, they often have a broader description for identity crime. This could have been driven from government initiatives for defining identity crime labels over time.[38]

Table 4 illustrates a sample of the rich responses received from the various US Federal and State Attorney Generals and US Statistic Bureaus. In Table 4 the feedback correspondence from Montana describes clearly the issues this paper is endeavouring to rectify. They point out the divergence and evolution of all groups; that for index crimes 'theft' is the highest rank in their crime classification but that under the Montana Incident-Based Reporting Scheme identity theft is categorized as a 'fraud' thereby potentially inflating fraud levels. Table 6 illustrates the various modes of researcher and legal definitions of identity crimes across different countries over time. In Australia, government and law enforcement have agreed on the following standard terminology: "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".[39] However, Australian legislation does not in the main use this terminology (see Table 5), due to concerns over limitations related to legal definitions of theft.[40]

The US federal government led the way in defining identity theft by way of legislation in the form of Identity Theft and Assumption Deterrence Act (1998) (see Table 6). This Act was introduced in order to mitigate the economic cost to victims, both entity and individual, by making identity theft a crime with substantial penalties in the form of fines or jail as a deterrent to future perpetrators. All US States subsequently followed this lead. We argue that the assumption part of the US Identity Theft and Assumption Deterrence Act (1998) identity theft definition is not identity theft but identity deception (see Table 5). We show that identity deception is a clearer referral, encompasses all similar labels, has

[37] Sommer, P., and Brown, I. 2011. "Reducing Systemic Cybersecurity Risk. OECD/IFP Project on "Future Global Shocks", January, pp. 1–121.
[38] See, The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) received Royal Assent on 12 December 2006. In the US a similar law is; Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001.
[39] Council of Australian Governments Agreement to a National Identity Security Strategy 2007, p. 3.
[40] See e.g., Steel, A. "The True Identity Of Australian Identity Theft Offences: A Measured Response Or An Unjustified Status Offence?" 33 (2010) University of New South Wales Law Journal 503–531.

Table 6 – Computer, cyber, and identity crime definitions (Researcher and legal).

Author	Region	
		Computer crime
Furnell 2002	UK	A crime in which the perpetrator uses special knowledge about computer technology (p. 21)
		Cybercrime
Furnell 2002	UK	A crime in which the perpetrator uses special knowledge about cyberspace (p. 21)
		Identity crime
ACPR 2006; MCLOC 2008	Australia	Refers to identity crime as: "offences in which a perpetrator uses a false identity in order to facilitate the commission of a crime"
COAG, Council of Australian Governments Agreement	Australia	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 (2007, p. 3).
UK Home Office Identity Fraud Steering Committee (2004)	UK	Classifies 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 (b) an existing (genuine) identity that has been altered to create a fictitious identity."
		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.
ACPR2006[a]	Australia	Identity fraud refers to the gaining of money, goods, services or other benefits through the use of a false identity
COAG 2007	Australia	"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" (p. 3).
		Identity theft
Oxford English Dictionary	UK	Identity theft (noun.), "the dishonest acquisition of personal information in order to perpetrate fraud, typically by obtaining credit, or loans, in someone else's name."
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 Transactions 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).
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 checks and to get new government documents such as driver's licenses and SIN cards
COAG 2007	Australia	"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" (p. 3)
		Identity deception
Wang et al., 2004	US	"Identity deception is an intentional falsification of identity in order to deter investigations" (p. 71)

a ACPR, The Australasian Centre for Policing Research (2006, p.9 footnote 7), makes the point that "the issue of intention (or the most appropriate fault element) may need to be considered in determining whether a criminal offense is involved in the use of a false identity".

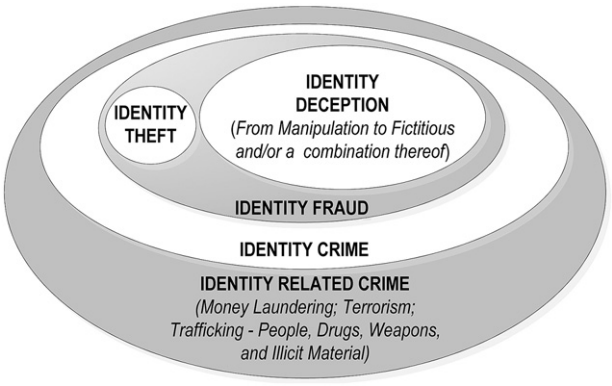

Fig. 1 – Conceptual model of identity definitions. Source: Jamieson et al., 2008.

precedence from a historical crime perspective,[41] academia,[42] and US State legislation (see Table 4).[43]

Identity deception (Table 1) is the rapidly growing phenomenon where fraudsters create identities and then steal goods and services from businesses (i.e. identity fraud). According to ID Analytics, Inc., identity deception accounted for about 85 percent of identity frauds compared to 15 percent for identity theft.[44] Those experiencing this phenomenon appreciate its far-reaching consequences versus those falling under the sub-class of identity theft.[45] Wang et al. describe their different criminal identity deception categories that fall under their labels of name, residency, identity and date-of-birth of deception, and each has sub-categories.[46] In Wang et al.'s identity deception taxonomy, reference to any identity crime act or event to obtain by a perpetrator proof of identity (POI) documentation or personally identifiable information, PII (personal identifying numbers, PIN or passwords), other than by identity theft methods may be more accurately classified as identity deception (see Table 1).[47] The basic premise of an identity theft act is that the perpetrator steals an individual or entity's POI or PII. Thus all other methods such as inventing, falsifying, altering or fabricating are classified as identity deception.

In mid 2008 the Australian Bureau of Statistics published the results of a personal fraud survey that asked questions to measure various types of identity crime incidents.[48] The publicly available results are at a reasonably high level across what we term the identity crimes sub-classes, in order to maintain survey respondent anonymity. A year after release of the data to the public, researchers who meet ABS research criteria could apply to access the data at more granular levels than was made public. We gained access to the data at a more atomistic level and made various integrity checks. For brevity and to maintain respondent anonymity, we reclassified and consequently recalculated the data at the publicly available level following our Table 1 (identity crime definitions and classes). This better ensured that results could be replicated by others.[49]

The identity crime portion of Fig. 3 identity fraud under the ABS classification is 3.1% with 499,500 victims made up of 124,000 identity theft victims (0.8%) and 383,300 (2.4%) credit or bank card fraud victims. The remainder are victims of personal fraud or scams.[50] However, using our definitions and classifications, phishing (57,800 victims or 0.4%) is an identity crime method (taxon), specifically it is grouped within the identity deception class that may cause identity fraud or be part of a related identity crime. In Fig. 2 we show the reclassified identity crime components that constitute the identity fraud portion (now 557,300 victims or 3.5%) of the ABS Personal Fraud Survey and the corresponding number of victims in each class where they can be categorically shown without ambiguity at this domain level. The broken uni-directional lines in Fig. 2 from 'credit or bank card fraud' to identity deception and identity theft are because at this level we cannot say the exact amount apportioned to either class, but we know over half of the new identity fraud victims are caused by this fraud (383,300 or 2.4%). We could apportion the 383,300 victims to identity deception and identity theft based on prior findings of 85 percent and 15 percent respectively,[51] but again this would not be accurate.

5. International context

The *Council of Europe's Convention on Cybercrime* ('*Convention*')[52] is the only binding international treaty on cybercrime. The *Convention* was negotiated and written in the earlier days of cybercrime – the late 1990s – with a final draft introduced in 2001. The *Convention* entered into force on 7 January 2004.

The *Convention on Cybercrime*, an agreement between member nations of the European Union is the only international agreement in the area of cybercrime. It is unique in that it is open for signature by non-European member states. The United States, Canada, Australia and Japan have all signed the *Convention*, with the United States also ratifying.

The *Convention* may be divided into three key divisions: substantive law, procedural requirements and international cooperation. All signatories to the *Convention* must criminalise certain activities.

The *Convention* creates four main categories of substantive offences:

[41] Stephan, see note [32].
[42] Chen, see note 4.
[43] Michigan or Indiana.
[44] ID Analytics. 2007. "US Identity Fraud Rates by Geography", ID Analytics, Inc. February, pp. 1–12.
[45] Chen, see note 4.
[46] Above note 4.
[47] See note 4.
[48] Above note 15.
[49] McKelvey, B. 1978. "Organizational Systematics: Taxonomic Lessons from Biology", Management Science (24:13), pp. 1428–1440.
[50] Above note 15.
[51] See note 39.
[52] Seger, A. 'The Convention on Cybercrime – Meeting a Global Challenge' (Speech delivered at the AusCERT Asia Pacific Information Security Conference 2008; Gold Coast, 19 May 2008); *Convention on Cybercrime*, opened for signature 23 November 2001, 2296 UNTS 167 (entered into force 1 July 2004) ('*Convention*').

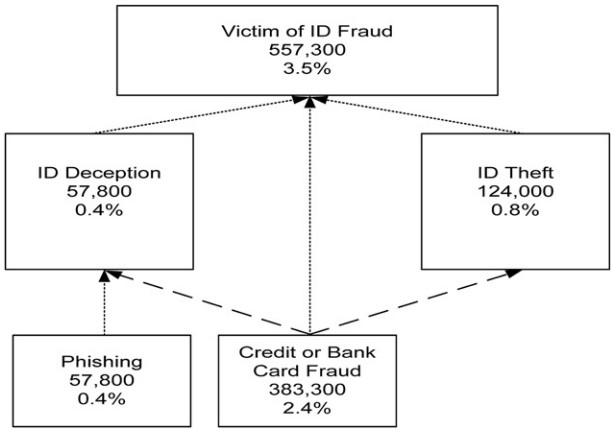

Fig. 2 – Identity crime Reclassification of ABS Fig. 2 personal fraud survey. Source: Australian Bureau of Statistics (2008, p. 7). Note: 'Credit or Card Fraud' methods (if caused by identity crime) should be apportioned to identity (ID) deception sub-class or identity theft sub-class. 'Phishing' is an identity crime method belonging to the identity deception sub-class.

1) offences against the confidentiality, integrity and availability of computer data and systems, comprising interference and misuse of devices;
2) computer-related offences such as forgery and computer fraud;
3) content-related offences, in particular the production, dissemination and possession of child pornography; and
4) offences related to infringement of copyright.

The *Convention* also addresses the procedural aspects of cybercrime. The main categories here are:

1) expedited preservation of stored computer data;
2) expedited preservation and partial disclosure of traffic data;
3) production orders;
4) search and seizure of stored computer data;
5) real-time collection of traffic data; and
6) interception of content data.

Finally, the *Convention* contains provisions relating to international cooperation. While some of these provisions are contentious, the *Convention* allows a certain amount of flexibility in terms of how a nation might negotiate some of the issues. These may broadly be categorised as:

1) extradition;
2) mutual assistance; and
3) designation of a 24/7 network contact.

Although the Convention criminalises computer-related offences and fraud, it does not specifically criminalise identity theft.

Alexandr Seger, Head of Economic Crime Division, the Council of Europe has spoken on the issue of identity theft stating:

> *"It is nevertheless worthwhile to continue the discussion as to whether in addition it is necessary to criminalise identity-theft as a separate offence or to develop a separate national instrument on the criminalization of identity theft in general, … , or whether the full use of the existing legal framework and a stronger emphasis on prevention would serve the purpose."*[53]

One significant disadvantage of not specifically including identity theft in the Convention is the inability to take advantage of the cooperative procedural elements such as cooperation with overseas law enforcement, real-time data collection, preservation of data, and immediate designated 24/7 points of contacts. As we have seen in this paper, identity theft is often retro-fitted into poorly-suited frameworks, or the individual is charged with a less relevant offence. A coherent and harmonized criminalization of identity theft as a separate offence (whether this is achieved through a separate international treaty or as a protocol to the existing *Convention*) would be beneficial.

6. Contribution, implication and limitations

Researchers and practitioners reviewing law enforcement practices may currently find it hard to scope, conceptualize, and understand the causal factors influencing the real underlying identity crime classes, as the definitions, taxonomies, classes and names adopted are non-standardized and have differing meanings especially across jurisdictions. There are currently few instances where there is common terminology used, that researchers can use with confidence in developing models that would help to predict and explain identity crime behaviour. This study makes a contribution to IS security via identity crime definitions and also contributes to other IS related disciplines for classifying crime incidents. Benefits for practice will flow from research accuracy facilitating clearer mandates and policy from governments directing monies for mitigation based on robust metrics. A limitation of this research is the limited access to data in most instances because collection of data and statistics on identity crimes are only just beginning to be collated and released.[54] While these definitional and classificatory outcomes may contribute to better research outcomes and practice policies, caution is required as we do not wish to make casual inferences.

7. New identity crime and future research

Legal definitions of crime are developed and amended by legislation. Such legislation often seeks to describe a prohibited behaviour in ways analogous to existing crimes, but legislators can struggle to find the best way to describe

[53] Seger, A., "Identity Theft and the Convention on Cybercrime" (2007) UN ISPAC Conference on the Evolving Challenge of Identity-Related Crime, Courmayer, Italy, available at http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/documents/reports-presentations/567%20UN%20id%20theft%20and%20CCC_en.pdf.

[54] Goode, above note 1.

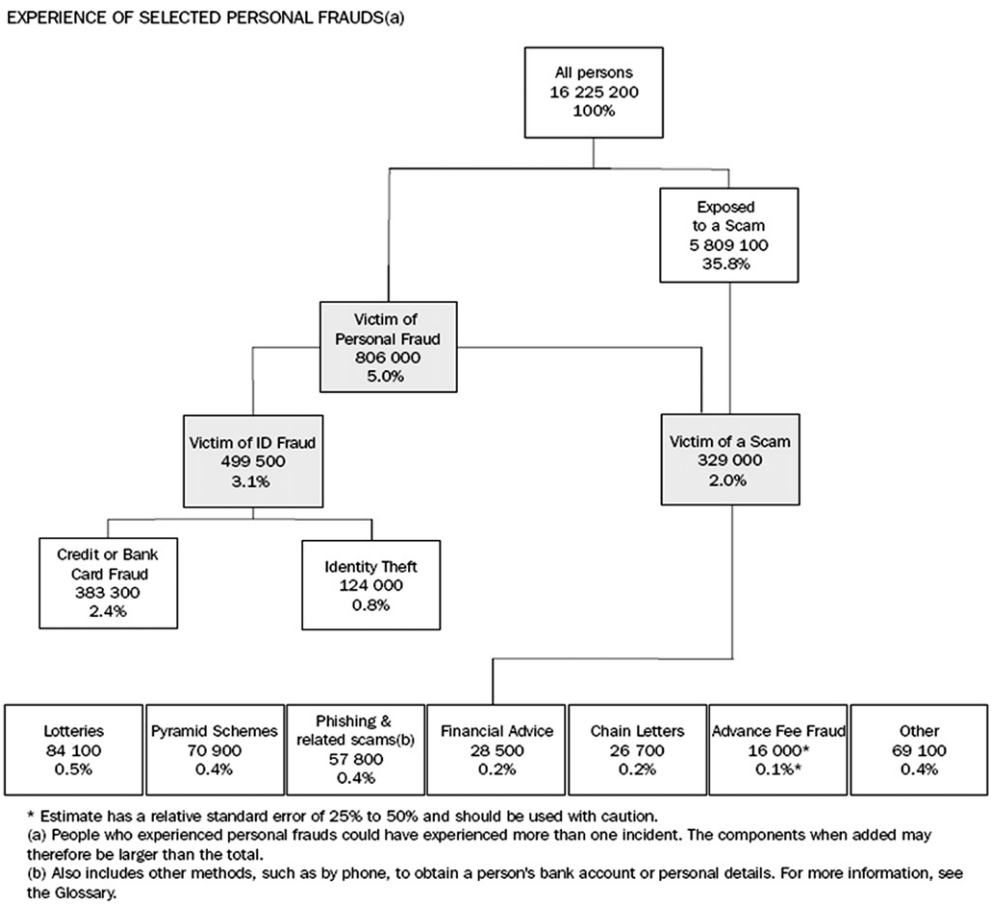

Fig. 3 – Australian Bureau of Statistics (2008) personal fraud survey classification. Source: Australian Bureau of Statistics (2008, p. 7).

evolving phenomenon. Identity fraud as a term and concept in its formative stages was often presumed to be identity theft and visa versa. However, identity theft is caused by individuals or organizations identities (or tokens) being stolen and is an enabling precursor to identity fraud. The boundaries of identity fraud and identity theft are now better defined.[55] The absence of specific identity crime legislation could be a cause of perpetrators not being convicted of identity crimes but rather under other specific entrenched law such as benefit fraud, or credit card fraud (or stalking; see Table 4). In crime management (IS) this means metrics overlap causing bias. On the other hand to redefine all frauds involving some degree of false identity as identity crimes may create the opposite bias. What is clear however is that there is significant advantage to a clear set of offences separately prohibiting behaviours amounting to identity theft and identity deception as precursor offences to other specific result oriented offences such as bank and benefit fraud.

We argue that the IS artefacts resulting from the collection, collation, storage and retrieval of identity crime research data and that the accumulation, refinement, and critical analysis of results should be greatly simplified by the availability of a dependable identity crime management IS classification scheme. Our discussion of identity crime evolution gives consideration to other areas of technology and crime that may have further impact on identity crime in the future.[56] Law enforcement, in general, takes the policy lead from government while constrained within a set of boundaries enacted by legislation, public harmony (voter empathy), and/or economic considerations. Sectors within law enforcement look forward to successful prosecutions of perpetrators of identity crime by the public prosecutors as an accomplished operation. Successful identity crime prosecutions act as a general deterrence to other identity crime perpetrators. Getting the major identity crime definitions and classes correct will ensure that prosecutions and sentencing procedures will be conducted without errors, according to the crime committed[57]; as well as correctly directing resources to well defined identity crime classes where they are most

[55] Sproule, above note 6.

[56] Bigelow, above note.[11] Orlikowski, above note 6.

[57] Mennens, A., De Wever, W., Dalamanga, A., and Kalamara, A., Kazlauskaité, G., Vermeulen, W., and De Bondt, W. (Eds.). 2009. Developing an EU Level Offence Classification System: EU Study to Implement the Action Plan to Measure Crime and Criminal Justice (34), Maklu, Antwerp, IRCP-Series. Vermeulen, G., and De Bondt, W. (Eds.). EULOCS. The EU Level Offence Classification System: A Bench-Mark for Enhanced Internal Coherence of the EU's Criminal Policy. IRCP-series, (39), Maklu, Antwerp, 2009.

needed.[58] Our research supports and commends efforts to devise and promote the use of a coherent identity crime classification framework via identity crime management IS for identity crimes within and across jurisdictions.[59]

A coherent identity crime classification framework could be achieved by the reinforcement around identity fraud, the laws could be fine-tuned and amended, or new identity crime laws could be introduced. Based on our findings in this study, we promote a combination of all three. Enforcement of existing identity fraud law is important, as is the education and prevention of such fraud. It is equally important that existing laws be fine-tuned in a manner which better relates to IS management systems or vice versa. Lastly, the introduction of a separate identity theft provision that was agreed to by members of the *Convention on Cybercrime* C would be beneficial.[60]

Rodger Jamieson (*r.jamieson@unsw.edu.au*), **Lesley Pek Wee Land** (*l.land@unsw.edu.au*), **Greg Stephens** (*g.stephens@unsw.edu.au*) & **Donald Winchester** (*d.winchester@unsw.edu.au*) *are members of The Australian School of Business, School of Information Systems, Technology and Management;* **Alex Steel** (*a.steel@unsw.edu.au*) & **Alana Maurushat** (*a.maurushat@unsw.edu.au*) *are members of the Faculty of Law; all of University of New South Wales, Australia; and* **Rick Sarre** (*Rick.Sarre@unisa.edu.au*) *is a member of the School of Commerce of the University of South Australia, Australia.*

[58] Brennan, T. 1987, "Classification: An Overview of Selected Methodological", Crime and Justice (9), pp. 201–248. Goode, above note 1. Kraus, above note 23.

[59] Sproule, above note 6; Stephan, above note 32.

[60] For analysis of the issues relating to such enactment in domestic contexts see above note 40.