2007

Identity Fraud: The Player Landscape in Australia

Rodger Jamieson
University of NSW, Australia, r.jamieson@unsw.edu.au

Greg Stephens
University of NSW, Australia, g.stephens@unsw.edu.au

Donald Winchester
University of NSW, Australia, d.winchester@unsw.edu.au

Identity Fraud: The Player Landscape in Australia

Rodger Jamieson, Greg Stephens, Donald Winchester
University of NSW, Australia
+61 2 9385 4414
{r.jamieson, g.stephens, d.winchester}@unsw.edu.au

Abstract

This paper investigates and categorises players in the identity fraud landscape in Australia. The player categories include: government and non-government proof of identity (POI) issuers and users; law agencies; the perpetrator; target organisations; solution providers and experts; the media; and community interest groups. The various interactions and collective arrangements between these organisations within and across sectors are important for several reasons. Firstly, in Australia, participants and identity crime perpetrators usually need a 'set' of POI documents which sum to at least 100 points in order to open accounts or receive benefits. The POI gathering sequence is referred to as the 'circularity effect' of acquiring POI documents. Secondly, perpetrators attack the 'weakest link' across a targeted sector and within targeted organisations. A contribution of this paper is to educe how organisations, in an IS context, through knowledge management (KM), knowledge sharing, sense-making, and organisational learning, from within and across sectors, can collectively combat the identity crime phenomenon.

Keywords

Information Systems, Organisational Learning, Knowledge Management, Sensemaking, Identity Fraud and Related Crimes (Terrorism, Trafficking, Money Laundering)

Introduction

This paper addresses the critical issue of how organisations cooperate to make sense of and learn from the targeted attacks from perpetrators of identity fraud and related crimes (money laundering, terrorism, trafficking), to mitigate losses. Identity fraud refers to the "gaining of money, goods, services or other benefits through the use of a false identity" (Australasian Centre for Policing Research 2006, p.9).This paper aims to clarify the identity fraud player landscape and the interactive relationship between groups of players (i.e., inter-organisational and inter-sector; see Wiley, 1988). Together, the participants (excluding perpetrators) are actors in the community of 'identity guardians' through the security and privacy of our public, confidential or sensitive information - where 'identity' means an individual's or entity's own proof of identity (POI) documentation and associated personal identifying information (PII), eg. a password for bank account access. The POI detail includes biometric, attributed, and biographical characteristics. Biometric characteristics are mostly fixed and stable over time; finger prints, retina, voice, signature and facial patterns are representative of this category. Attributed characteristics include our names and biographical characteristics, of which education and employment detail are examples. Attributed and biographical data change and accumulate over ones life. Where and how perpetrators acquire illegitimately issued and fraudulently obtained POI or PII is paramount for prevention strategies and policies. Without mitigating the perpetrators' attacks, the integrity and trust of the whole Australian Identification System (AIS) is at risk. Information Systems (IS), with the advances in technology, play a significant and growing role in the collection, storage, sharing and analysis of identity information.

Recent identity fraud related surveys from the United States (ID Analytics 2007) and United Kingdom (CyberSource 2007) show the diverse nature of the identity fraud phenomenon within communities. These surveys have drawn the public and associated political attention away from perpetrators and towards the victims of identity crime. They inform the community through diverse media alerts about needed safeguards to protect the public from the threat of identity crimes. The cost of identity fraud in Australia was estimated at A$1.1 billion in 2002 (Cuganesan & Lacey 2003) and "up to US$2 trillion globally by the end of 2005" (The Fraud Advisory Panel 2003, p.1). As a consequence, identity crime may have a discouraging effect on the further adoption and uptake of e-commerce/IT/IS (hereafter IS). Reasons include privacy, security, lack of trust, economic loss, emotional stress, and reputational losses suffered by victims and targets – individuals and organisations. Industry and government are now taking the identity crime phenomena seriously. Anonominity granted to identity crime perpetrators through the Internet means that jurisdictional borders are not a restriction for perpetrators of identity fraud acts when selecting target organisations. Framed in this context, we are motivated, to extend earlier sensemaking research of knowledge management (KM) in organisations (Cecez-

Kecmanovic 2004; Cecez-Kecmanovic & Jerram 2002) to an inter-organisational and sector levels (figure 1) and learning (figure 2) as our conceptual framework for the identity fraud players' landscape (figure 3). Sensemaking is "a motivated, continuous effort to understand connections (which can be among people, place, and events) in order to anticipate their trajectories and act effectively" (Klein, Moon & Hoffman 2006). "Literally, it means the making of sense" (Weick 1995, p.4). The next section reviews sensemaking and learning models in organisations, followed by our sensemaking model extension where we add two knowledge levels. We then explain our methodology. Our classification of identity fraud players is then presented and discussed with resulting implications and limitations, followed by our conclusions and future research agenda.

Background to Sensemaking and Learning Models in Organisations

The sensemaking model of knowledge in organisations (Cecez-Kecmanovic 2004; Cecez-Kecmanovic & Jerram 2002) identifies four types of knowledge, corresponding to four sensemaking levels (Wiley 1988), individual, inter-subjective or collective, organisational, and knowledge embedded in culture. The four identified types of knowledge, corresponding to specific sensemaking levels are shown in figure 1 and their interactions shown by directional arrows. Cecez-Kecmanovic & Jerram (2002, p.896) posit that the first level '*individual knowledge*' "involves a person's values, believes, assumptions, experiences, and skills, etc. that enable the individual to interpret and make sense of the environment, his/her own actions and the actions by others". The second level, '*inter-subjective or collective knowledge*' "represents shared understanding that emerges through social interaction". The third level, '*organisational knowledge*' "denotes generic meanings and social structures that emerge in and reproduce an organisation". Their fourth level, '*knowledge embedded in culture*' "assumes a stock of tacit, taken-for-granted convictions, beliefs, assumptions, values and experiences that members of an organisation draw upon in order to make sense of a situation and create meanings at all other levels".

Organisational learning occurs "when members of an organisation change their shared assumptions and beliefs and in turn change the range of their behaviour and enhance their capacity to act" (Janson, Cecez-Kecmanovic & Zupancic (2007, p.4). They show how the role of IT systems in organisational learning depends on the nature of learning (single-loop, double-loop or triple loop) in a longitudinal study of a Slovenian diversified manufacturer. The learning loops are briefly explained with examples relevant to preventing, detecting, or deterring identity fraud in an organisation:

- *Single-loop learning*, "involves adaptive responses: measuring an organisation's performance, comparing it with its stated goals and taking corrective action to close the gap". For example, single-loop learning comprises adjusting a security system to make sure that system meets security standards;
- *Double-loop learning* "involves evaluating and changing organisational goals, organisational strategies and mental maps". For example, if a system is hacked with the loss of data, a firm is required to rethink its security and develop new mental maps to allow the firm to change its security strategy.
- *Triple loop learning* "occurs in response to a realisation that existing mental models and ways of organisational learning no longer suffice". For example, inventing a new system or process such as, profiling using a computer immunology method to identify and prevent identity fraud perpetrator attacks (refer Janson, Cecez-Kecmanovic & Zupancic (2007, pp 6-7) and references therein for more explanations of learning loops).

As a means to better understand learning we make a connection between organisational learning, knowledge management, and sensemaking with the aid of the sensemaking model of knowledge in organisations and the nature of the organisational learning models described so far. To facilitate this with the data in our study we add two levels to the sensemaking model of knowledge in organisations.

Sensemaking and Learning Models of Knowledge across Organisations

The sensemaking model of knowledge in organisations we use has been used in IS - for example in case and field study in areas of retail, investment banking (both longitudinal, Cecez-Kecmanovic 2004) and tertiary education (Cecez-Kecmanovic & Jerram 2002; Cecez-Kecmanovic 2004). We propose an extension of levels within the sensemaking model of knowledge in organisations to better fit our data. We extend the four levels of knowledge outlined earlier and illustrated in figure 1 to incorporate '*inter-organisational knowledge*' and '*intra- and inter-sector knowledge*' (both new levels can be across jurisdictions or national boundaries for private industry or government agencies) that will correspond with additional levels of sensemaking. We now describe these two outer levels (level five and level six):

1. *Inter-organisational knowledge* brings to an individual organisation, shared knowledge from another or many organisations participating individual(s) through their social interaction (levels 1 to 4). Also brought to the inter-subjective organisational exchange are accumulated interpersonal skills**,** formal training, heuristics, nuances, organisational reputation and power, implicit and explicit organisational imposed confidentiality restrictions that extend (and limit) tacit and dynamic exchanges, that enhance knowledge and sensemaking of the engaging exchanges in the subject matter under discussion.
2. *Intra- and Inter-sector knowledge* reaches across the previous outlined knowledge and sensemaking levels from individual to inter-organisation knowledge. Individuals engaging at the sector level will exhibit a vast array of skills acknowledging her or his elevation of engagement including critical thinking, foresight, insight, strategic, and holistic problem solving comprehension capabilities.

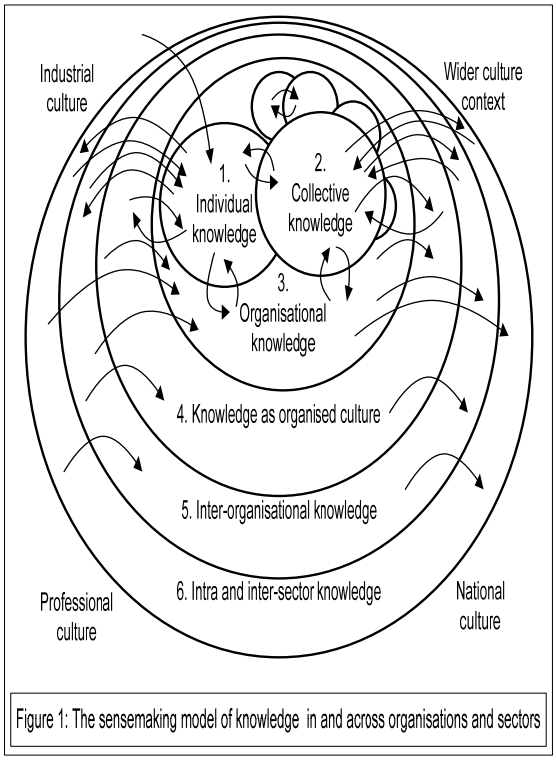

Figure 1: The sensemaking model of knowledge in and across organisations and sectors

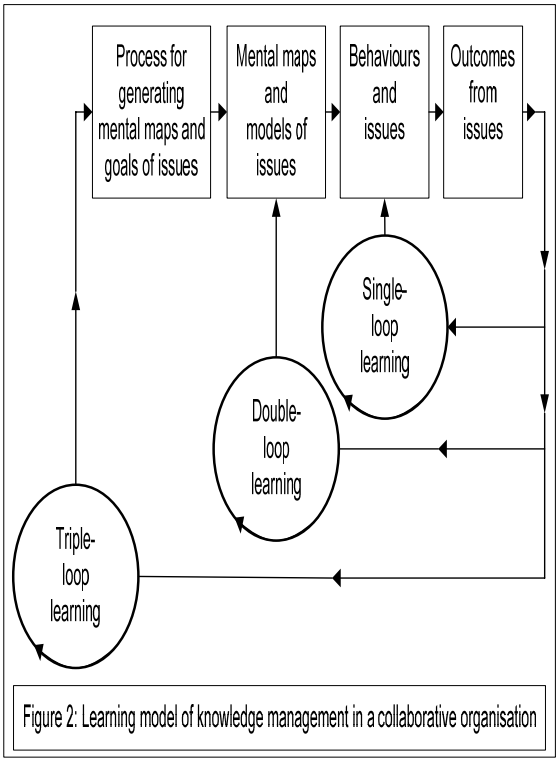

Figure 2: Learning model of knowledge management in a collaborative organisation

The focus of this study for level five and six is making sense of and learning (by acting) and thereby making more headway to solving the identity crime crisis experienced by each contributing organisation through collaborating. Individual knowledge may come from a multitude of disciplines within collaborating organisations as exhibited by the roles of interviewees in table 1. In Australia, inter-organisationally, within and across sectors this could be facilitated by industry associations, peak bodies, and government committees made up of inter-agency and private sector participants.

Methodology

The aim of this research is to determine the main categories of identity fraud players (in Australia) and how they interact with one another to deter, prevent and detect identity fraud perpetrators. We hypothesise that target organisations within a sector and across sectors that cooperate, coordinate, communicate and learn (Janson, Cecez-Kecmanovic & Zupancic 2007) through interacting and using knowledge management and sensemaking (Cecez-Kecmanovic 2004; Cecez-Kecmanovic & Jerram 2002) will have a higher probability to combat identity fraud. The research design identifies, from the literature, some existing identity crime players (Cuganesan & Lacey 2003; Tan 2002; Wang, Yuan, & Archer 2006). Semi-structured interviews were undertaken with experts from industry and government groups, which were identified from earlier empirical studies (Cuganesan & Lacey 2003; Wang, Yuan, & Archer 2006). Interviewees from these groups are representatives of the major organisations targeted by identity fraud perpetrators.

First, a pilot interview evaluated the proposed questions for their suitability, coverage and to determine interview duration. The interviews were recorded, transcribed, coded and analysed using NVivo qualitative data analysis software (QSR International). The organisations and interviewee roles are set out in table 1. At the top level our interview protocol questions followed several main themes including: what is identity fraud in your organisation; managing identity fraud; identity fraud reporting; and identity fraud issues and research. Individual

questions are not included for brevity. Our approach, in order to gather deeper insights from the interviews, includes participant quotes (in *italics*) of challenges, issues and mitigation strategies adopted by interviewees' organisations.

Table 1: Participant Interview Category and Role Key

Participant	Participant Category	Participant Role
1	Bank 1	1. Head of Fraud – Policy & Strategy
2	Bank 2	1.Chief Manager Operational Control 2.Fraud Management
3	Bank 3	1. Manager Research & Intelligence 2. Intelligence Officer 3. Business Services 4. GM Strategy & Security Risk
4	Licensing Authority 1	1. Licensing Policy & Projects 2. Manager of Finance & Operations Audit 3. Investigations External Fraud
5	Licensing Authority 2	1. Manager
6	Telecommunications 1	1. Fraud Risk
7	Government Agency 1	1. Compliance, Integrity & Documentation Examination
8	Government Agency 2	1. Detection & Review 2. Manager 3. Investigations ID Fraud Specialist 4. Manager 5. Quality POI team 6. Manager
9	Government Agency 3	1. Director Internal Audit 2. Internal Issues Manager 3. Program Delivery 4. Manager 5. Manager
10	Government Agency 4	1. Deputy CEO – Corp Services and Regulatory Issues
11	Government Agency 5	1. Client Account Management
12	U.S. Criminologist	1. Academic – Professor

Model Categorising Players in the Identity and Identity Fraud Landscape

The identity fraud player landscape is larger and involves more people and organisations than just the perpetrator(s). Figure 3 was derived from the previous literature (refer Wang, Yuan, & Archer 2006; Tan 2002; Cuganesan & Lacey 2003) and then modified from the results of the interviews. This model shows our categories of main players and their interactions, shown by the lines between them. The interactions convey the merits of knowledge sharing, making sense of this sharing and learning. These findings were the grounding for the extensions to the adapted models in figure 1 and figure 2. We did not interview players in media or community organisations, but we did discuss the media and community organisations with interviewees and their interactions to elicit their perspectives. Responses from interviewees in table 1 provide our scope. Most interactions between the categories are centred on POI and entities trying to mitigate perpetrators' identity frauds.

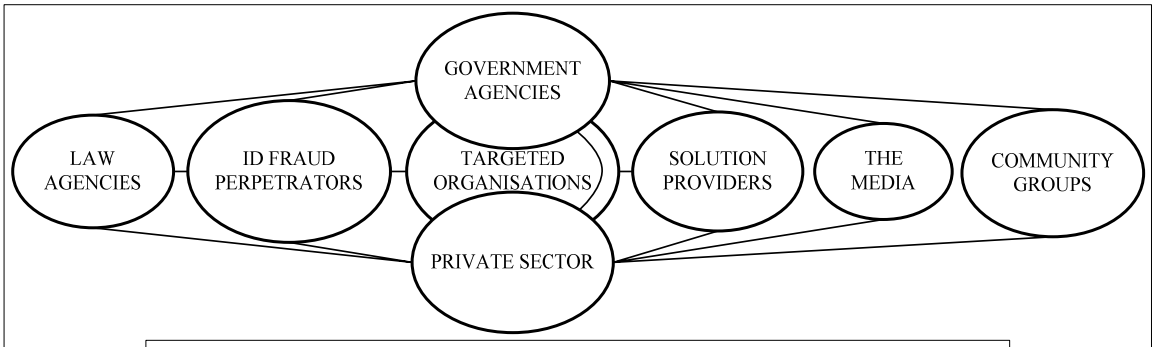

Figure 3: Participants in the Identity Fraud Player Landscape and their Relationships

Government Agencies

Government agencies in figure 3 interact with all other categories. They are diverse and include: legislators and regulators; welfare (POI issuers and users); and research. Many government agencies are a monopoly within a country - for example, immigration, tax, and therefore collaboration within a country is often across sectors. In this case within sector collaboration takes place across country jurisdictions e.g., immigration. Yet with road

transport, and births, deaths and marriages, there may be an agency in each state, with sector cooperation occurring within a country but also across state jurisdictions.

Legislators play key roles in writing new laws and amendments for identity fraud and related crimes nationally and internationally. The State of South Australia is the only state to enact identity fraud related legislation (in 2004) therefore making identity theft a crime in that state. However, the State of Queensland has just recently introduced an identity fraud bill. The Federal government also has documentation on identity fraud that has just completed the public discussion phase. The Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (which replaces the Financial Transaction Reports (FTR) Act 1988) requires Australian financial institutions, to undertake certain steps when dealing with customers who transact cash over A$10,000 or who act suspiciously. "*Most people know about the 100 points (POI) system. You need your driver's licence, a couple of credit cards, and your Medicare card to add up to 100 points*" (Participant 10). These POI documents form the base set of the AIS documents issued and used by government agencies and are an inter-organisational link. "*You explain in real terms the 'circular path', how people use documents to get one and then the other, so we rely on things like passports, immigration papers and so on. The date of birth is one key identifier*" (Participant 4:1).

In Australia, there are a number of government agencies (see Cuganesan & Lacey 2003, Table 5, 6 and 12, pp.49-51 and p.70.) that issue and use POI. At the Federal level for example, Centrelink for pensions, Department of Foreign Affairs and Trade for passports, Department of Immigration and Multicultural and Indigenous Affairs issue visas and citizenship certificates, and the Australian Securities Investment Commission issues company registrations. State or Territory issuers and users include road transport authorities, Birth, Death and Marriage registries, and Fair Trading Offices (Business Name Registrations). Participant (8:6) explains their organisation's approach "*our particular model is based on tier levels, depending on the POI document, and degree of risk. We've gone, rather than sticking to primary and secondary* (identification) *that a lot of other agencies still have, to a points system. So basically it's a risk-based model. We know if we do some work for Participant 11, which will be a tier 3, which is our top tier, we can meet their requirements quite readily*".

Legislators also set up organisations to research identity crimes. The Australian Institute of Criminology (AIC), a Commonwealth statutory authority, operates under the Criminology Research Act 1971. The functions of the AIC include: conducting criminological research; communicating the results of research; conducting or arranging conferences and seminars; and publishing material arising out of the AIC's work. Other organisations set up similarly with a research component include: the Australian Centre of Policing Research (ACPR); the Australian High Tech Crime Centre (AHTCC); and the Australian Transaction Reports and Analysis Centre (AUSTRAC). The ACPR liaises closely with other national police services, such as the National Institute of Forensic Science, the National Crime Statistics Unit, the Australian Institute of Police Management and CrimTrac. The ACPR is an active member of a number of government agency and private sector working groups and committees (e.g., the Australian Bankers' Association Fraud Task Force, the AUSTRAC Proof of Identity Steering Committee and the AFP Opal Group) that address identity crime issues. The Australian High Tech Crime Centre (AHTCC) consists of representatives from private sector and government. The AHTCC's brief is to combat serious and complex high tech crimes, especially those beyond the capability of a single jurisdiction. An integral part of the AHTCC is the Joint Banking Finance Sector Investigation Team (JBFSIT) combating internet banking fraud. AUSTRAC was established under section 35 of the FTR Act. AUSTRAC has many partners, such as the Australian Crime Commission, Australian Customs Service, and the Australian Federal Police. Government agencies show many interactions and collaboration across organisations, and within and between sectors.

Private Sector

The dominant non-government (industry) POI users are those organisations targeted by identity fraud perpetrators, such as financial institutions (banks), utility organisations, and retailers. Non-government POI document issuers include all organisations that as 'part of their normal business' issue documentation with personal identifying information (e.g., name, date of birth, address, age). While organisations are assumed to have a 'duty of care' when holding employees or customers PII most organisations stipulate or consider the gathering of this information is for a specific purpose e.g., a bank statement or utility bill is a record of a customer's spending habits and account of their liabilities not POI points. The identity fraud perpetrator directly targets the weakest link in the AIS, seeking to obtain legitimately issued but fraudulently obtained POI documentation. The process is made easier for the perpetrator with the anonymonity of a victim's POI and PII details and organisations who operate in isolation or in another jurisdiction. "*These kinds of displacement theory displacement phenomenon … it relates to this whole issue (identity fraud) – there is this constant thrust and parry*" (Participant 12) to find the weakest link.

An extract list of non-government POI issuers and their documents that contain various PII are discussed next (refer Cuganesan & Lacey 2003, Table 5 and 6, pp.49-51). Educational organisations (Secondary, Tertiary and Institutes) issue certificates of qualification (educational and trade qualifications), student identity cards,

certificate or statement of accomplishment or enrolment and letters (POI should not be more than 12 months old) from principals that are recognised as POI when issued from bone fide educational institutions (Smith 2006). Financial institutions under the Australian FTR Act 1988 include Banks, Building Societies, and Credit Unions (e.g., Savings & Loans in the US). POI documentation issued includes current credit and debit cards or account cards or passbooks. Examples of utility organisations include telecommunication companies (also Internet Service Providers), electricity suppliers, gas suppliers, water service providers and councils. These organisations issue POI such as, statements (with current address) and accounts (not more that 12 months old) that are used by others as part of their POI processes. Health insurance and health fund organisations issue membership cards, statements and other documentation of payments that are used as POI by various government and industry organisations. Examples of other non-government POI issuers include: associations; groups; and peak bodies; libraries; clubs (e.g., League); unions and associations who also issue 'secondary' POI that form part of Australia's identification system, such as membership cards, statements and other documentation or payments.

Within the private sector the distinction between individual sectors is clearer with many banks, retailers, or utilities grouping in a sector. Feedback from interviewees suggested collaboration within a sector regarding systems or processes did not normally occur due to competitive advantage issues. However, when it came to combating new crimes such as identity crimes, organisations were openly cooperating. Inter-sector collaboration in the private sector was a newer innovation. A large amount of information sharing occurred with government agencies, especially law enforcement agencies, such as the Police.

Law (Enforcement) Agencies

Law enforcement, courts, and corrections systems are the focus of this section. One of the difficulties for law enforcement in combating identity fraud and related crimes arises from a unique feature of the crime pertaining to the legal jurisdiction responsible for adjudication of a crime. Confusion over who should investigate and prosecute leads to inconsistency in reporting and frequent lack of action. Identity crime raises issues such as, the adequacy of current legislative regimes, training for police and the community in prevention and response measures, and dealing with a range of victim-related issues, including legal standing or status and privacy restrictions or requirements. Government law enforcement agencies often collaborate with each other (e.g., see Government Agencies section) as well as with other government and industry organisations, associations, commissions and groups in order to combat identity fraud. For example, Participant 4(3) states, "*I've been put in place basically to allow the backdoor to be opened up slightly. To allow information flow to come through and to assist law enforcement agencies with evidence gathering and various checking. Quite a significant finding is that, with 80% of detection of people getting through the frontline is found through that particular process. We know that there are legitimately issued, fraudulently claimed licenses, and we collate points, and sometimes the real person's license is then cancelled. In an experimental stage at the moment, where if financial institutions suspect that they've got a fake license holder before them, and they can provide my area with a good quality copy of that particular document - so it's got to be able to see the image and they state why they think it's a fake document*".

Police in general and fraud squad members in particular interface with industry e.g., retailers and financial institutions (mostly banks), to try and stop identity crimes. Another example of when police work in conjunction with organisations is in remote areas of Australia. A real life situation in an Australia State is related by Participant 5(1), "*at a higher level State Transport and State Police both are working pretty closely both in the issuing of licenses in remote ... in major cities and towns around the State, State Transport has the function of doing the license issuing function, but in a lot of the smaller remote type areas State Police will act as our agent. So there is some close working links between us and State Police in that regard*". In an e-fraud environment, stopping perpetrators "requires law enforcement officers to move just as quickly (as the perpetrator) and demands unprecedented cooperation among a whole spectrum representing government, business and consumer groups not just from the place of the offence but across national or state borders as online transactions usually span different geographical borders" (Tan 2002, p.353). In Australia, the following judicial punishments are currently available in most jurisdictions for identity fraud and related crimes (money laundering, drugs, terrorism, immigration etc) caught under various legislation and amendments including, fines, restitution and compensation orders, forfeiture and disqualification (confiscation), unsupervised release (suspended, deferred, conditional sentences), supervised release (probation, community service, intensive corrections), custodial orders (either full time or periodic) (see Graycar 2000 p.12), immigration detention centres, and deportation. In the US, specific legislation has been introduced to deal with identity-related crime. The Federal Identity Theft and Assumption Deterrence Act of 1998 (18 USC 1028) makes identity theft a crime with maximum penalties of up to 15 years' imprisonment and a maximum fine of US$250,000. Australian government organisations investigate and refer serious breaches of the law to the Commonwealth Director of Public Prosecutions to consider for criminal prosecution. Several perpetrators have now been successfully prosecuted by government agencies, with their actions being viewed very seriously by the courts. A major part

of identity fraud and related crime deterrence is punishment delivered by a country's judicial system as set down by legislation. The role of correctional systems is to carry out the court imposed custodial sentences. In Australia correctional facilities include detention centres (DIMIA) and prisons.

Identity Fraud Perpetrators

We classify identity fraud perpetrators into four distinct categories (see, Jamieson, Stephens & Winchester 2007). The first is organised crime groups. "*Organised crime groups are usually sophisticated, networked and well resourced*" (Participant 4). "*In some of those cases the target audience receiving licenses was outlaw motorcycle gangs*" (Participant 5). "*A lot of this form is organised, particularly Asian syndicates (e.g., Triads)*" (Participant 1). The second category of perpetrators is sophisticated individuals or pairs, often specialising and proficient in certain methods of identity fraud acts. These sophisticated individuals are more likely to be traders in identity documentation and be part of an underworld network often in an e-commerce environment frequenting specialist sites to trade (chat rooms, blogs). An example, of a specialised method is phishing, where a perpetrator impersonates a trusted organisation, creating false emails and Web sites to steal personal information. A question posed was: do you have a feel for what ID fraud you're not detecting? A typical answer was "*probably the most sophisticated ones get through*" (Participant 8:3). The third category is the more opportunistic perpetrators. They will often obtain POI or PII through theft of mail, dumpster diving, or mail redirection. Over time they may (have to) become sophisticated, graduating to the second category. "*As a lot of the amateurs have been squeezed out (or caught)*" (Participant 1). The fourth category operates internally in the target as an agent of the organisation (includes: employees; contractors; and consultants). Employees have also been used by organised gangs to infiltrate an organisation. This requires far more vigilance and better controls to be in place in the target organisations (refer, Wang, Yuan & Archer 2006). While we identify four broad categories in our classification, we are unable to answer the generic question: what does an identity fraud perpetrator look like? There is no one answer. Perpetrators to-date has come from all walks of life and includes: males; females; rich; poor; and most ethnicities; locations; and age groups. Worse still, they are also collaborating as well.

Targeted Organisations

Perpetrators target both public and private organisations. Perpetrators target these organisations to obtain POI/PII and then using this illegally obtained information to by-pass security for an economic benefit – committing identity fraud acts. Target organisations to-date have predominantly been financial institutions – especially banks, utility organisations, retailers and government welfare agencies but include all sectors of economic activity (see Cuganesan & Lacey 2003). To counter these attacks the Australian government has set up committees and taskforces to tackle the identity crime issues. The Identity Crime Taskforce includes: Australian Federal Police; NSW Police; NSW Crime Commission; NSW Independent Commission Against Corruption; and the Australian Crime Commission. Private organisations weigh up the dollar amounts taken by the perpetrator against the recovery and remediation costs. For instance with banks, retailers and utilities organisations, "*there's a 'threshold effect' that takes place when systems get too over burdened with cases*" (Participant 12). In Australia in the mobile phones sector this threshold might be $50 per user's phone for example. "*The hacking incidents are where the excess usage is – the biggest one I've seen is just $900. That way exceeds anything else*" (Participant 6:2). "*The cost (loss) is basically rolled over … to the customer there's no gain to be made going through the criminal justice system*" (Participant 12). However, these small individual losses across 10,000 incidents amount to a significant total economic loss.

Within sectors, targeted organisations often meet and strategize how, as a group, to combat identity fraud with new systems. "*We turn up to these fraud forums … re the Telco sector and even with I-Me blocking a perpetrator's mobile is rendered useless within Australia. But organised crime will just send these things overseas*" (Participant 6:1). Personnel within targeted organisations (government and private sector) as members of groups, forums and associations gather intelligence through these intra- and inter-sector networks. "*We get some sort of feedback – areas of which I have been involved with include: Australian Bureau of Criminal Intelligence; the Australian … AusRoads Administration and Licensing Group; and Interagency Fraud Committee*" (Participant 4:3). For example, "*AusRoads in all their jurisdictions are tightening up their identity processes, so we are going to be adopting similar processes*" (Participant 5).

Solution Providers and Other Experts

Solution providers include technology organisations, researchers, industry associations, manufacturers, and standard setters of POI documents. In an IS context, solution providers are playing an increasing part in the identity fraud player landscape, due to the pervasive increase of the Internet and e-commerce as an attack channel and the innovations in IS related methods of attack. The link between targeted organisations and solution providers is grounded from interviewee organisations providing verification, credit and fraud checking

data services. With recent applications moving from delayed (24 hours) to real time or even where "*both systems* (run) *in parallel. Where the delayed system is used as a search database (knowledge management) from the outside – by law agencies*" (Participant 4). For example, "*we use credit bureau Baycorp products including Fraud Check and Decision Point - to check identity … also Hunter and VeriCheck*" (Participant 6:1). "*We use NEVUS, which is a national system allowing us to look at licensing information from NSW and other States*" (Participant 5). Researchers investigating solutions into identity fraud can be funded by government (eg., the Australian Research Council (ARC) grants) and/or industry. For example, the SEAR (Security, E-Business, and Assurance Research) group at University of New South Wales.

Industry experts include auditors, forensic accountants, and computer specialists. Often these professions have barriers to entry in the form of skill sets, and tertiary and professional examinations. Expert's skills are of increasing importance when organisations or their customers follow remediation processes. Solution providers interact with targeted organisations to reduce risks for their clients. An irony of being good at risk reduction is an "*escalation of criminal behaviour. You could create some more serious scenarios. Make it almost impossible to steal someone's ID through the Internet then they actually go kill someone to steal biometric data or whatever. But end up actually escalating the problem*" (Participant 12).

The Media

Media organisations may be owned by government or private organisations and include television, radio, newspapers and magazines. Often organisations, associations, peak bodies, and community groups, both publicly or privately operated have their own media sections and personnel who release information directly to members and the public via their websites or via the media. Television and newspapers have been the dominant mediums exposing identity fraud perpetrators in Australia over the last few years. Media coverage deals with public awareness, concern, educating and alerts, by generally informing them. On the other hand freelance and investigative journalists also play important roles by researching information below the 'spin' of the public or private organisation releasing initial information.

Other roles played by the media can include waging campaigns for (against) proposed legislation that might increase (restrict) access to data. The media are not bound by the Privacy Act 1998. There is "*this whole notion of where the public stands on it, it effects policy making and related issues. That notion of cultural diffusion is at work you could have a major problem. It's probably going to reach some critical level where it's going to enter the political arena. The issue of identity fraud is probably increasing in terms of public consciousness. One major debate that it has infiltrated is in acts of terrorism*" (Participant 12).

Community Groups

Community based groups, set up to mitigate identity crimes are backed by government or the private sector as outlined above, e.g., Australian High Tech Crime Center and Australia Bankers Association (ABA). Other collectives are privacy groups (e.g., Australian Privacy Foundation) who provide a balance in the debate for consumer protection for privacy and security of their identity information and rights from government and industry. "*It might be useful to have some market research on what the community thinks (about centralised identity databases)*" (Participant 4:1). To abate 'big brother' fears about the protection of POI and PII data (including images) systems for the country's citizens. "*A constraint on this system is that identity issuers and users rely on each others information – the 'circularity effect'*" (Participant 4:1). "*Another difficulty is that we have to operate within the parameters of privacy legislation. We have our own privacy officer. And he liaises with the NSW Privacy Commissioner*" (Participant 4:3). "*We're restricted by the Privacy Act and the Social Security Act*" (Participant 8:5). Legislation in Australia, US and other jurisdictions are receiving renewed attention due to recent data breaches and data matching programs of government and industry. "*I think that there is certainly a lot of data sharing and information sharing between agencies. But there are inhibitors on what we are allowed under our legislation to share and privacy considerations. We have to work within these parameters*" (Participant 7). "*There is the privacy commissioner who reminds us it is not mandatory in a lot of instances to quote your tax file number*" (Participant 11). In summary, checks and balances are important too. Information Systems (manual and automated) knowledge sharing is an example of how organisations are collaborating, monitoring, managing knowledge and learning through sense-making at the inter-organisational, intra and inter-sector levels.

Implications and Limitations

The implications for organisations that collaborate within and across sectors, industry and government are positive. The research has identified that through industry groups (e.g., AUSTRAC, Australian High Tech Crime Center including JBFSIT; ABA, i.e., banking groups fighting the same enemy), committees (AUSTRAC Steering committee, The Identity Crime Taskforce), research groups (AIC, SEAR) has drawn out that there is a

lot of sensemaking at our extended levels. Learning and associated actions were just filtering through at interview time mostly at the first-loop. A limitation of this study is that we did not interview perpetrators or players from community groups, the media, or solution providers - our scope was from the targets' perspective. Also the communities within different states and jurisdictions will differ across countries. However, we start the process within an Australian context. Our approach could also be adapted to other crimes or phenomenons that similarly require collective actions for mitigation.

Conclusion and Research Agenda

In this paper we have argued that to combat identity fraud perpetrators in an IS context, targeted organisations need to collaborate. Our approach sought to conceptualise the sense-making model of knowledge management in organisations (Cecez-Kecmanovic 2004; Cecez-Kecmanovic & Jerram 2002) and organisational learning (Janson, Cecez-Kecmanovic & Zupancic 2007) to an inter-organisational, intra and inter-sector context grounded from industry and government player interviews.

Feedback from industry experts determined that many organisations both public and private are collaborating to combat identity fraud perpetrators. There was evidence that target organisations who 'went it alone' became weak links in the Australian Identification System and were 'picked off' by perpetrators. Organisations both public and private that collaborated had better identity defenses through information sharing. The categorisation of participants in the player landscape and perpetrators will facilitate future prevention, and detection strategies, tools and solutions. Developing and testing profiling tools within and across databases in the IS space to combat this phenomenon is on our identity fraud research agenda.

References

Australasian Centre for Policing Research (ACPR) 2006, Standardisation of definitions of identity crime terms: A step towards consistency, *Commonwealth of Australia* (145.3), March, pp. 1-22.

Cecez-Kecmanovic, D., A sensemaking model of knowledge in organizations: a way of understanding knowledge management and the role of information technologies, *Knowledge Management Research & Practice* (2:3), 2004, pp. 155-168.

Cecez-Kecmanovic, D., & Jerram, C., A Sensemaking Model of Knowledge Management in Organisations, *ECIS* (June), 2002, pp. 894-904.

Cuganesan, S., & Lacey, D., *Identity Fraud in Australia: An evaluation of its nature, cost and extent*, Standards Australia International Ltd. Sydney, 2003.

CyberSource., Third Annual UK Online Fraud Report: Online Payment Fraud Trends and Merchants' Response, *CyberSource Corporation* (2007 Edition), 2007, pp. 1-20.

Graycar, A., Fraud Prevention and Control in Australia, *Fraud Prevention and Control Conference* 2000, (August), pp. 1-13. http://aic.gov.au/conferences/fraud/graycar.pdf.

ID Analytics., US Identity Fraud Rates by Geography February 2007, *ID Analytics, Inc*. 2007, pp. 1-12.

Jamieson, R., Stephens, G., & Winchester, D., An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts, *PACIS*, July, 2007, pp. 1-14.

Janson, M., Cecez-Kecmanovic, D., & Zupancic, J., Prospering in a Transition Economy Through Information Technology-Supported Organizational Learning, Info Systems Journal 2007 17, pp. 3-36.

Klein, G., Moon, B. & Hoffman, R.F. Making sense of sensemaking I: alternative perspectives, *IEEE Intelligent Systems*, 2006 21(4), pp. 70-73.

Saydjari, O., Privacy-Enabled Global Threat Monitoring, *IEEE Security & Privacy* 2006, pp. 60-63.

Smith, R., Identification Processes in the Higher Education Sector: Risks and Countermeasures, *Trends & Issues* (December:305), 2006, pp. 1-6.

Tan, H., E-Fraud: Current Trends and International Developments, *Journal of Financial Crime* (9:4), 2002, pp. 347-354.

The Fraud Advisory Panel., *Identity Theft: Do you know the signs? A guide for businesses and individuals*, The Fraud Advisory Panel London, 2003, pp. 1-24.

Wang, W., Yuan, Y., & Archer, N., Identity Theft: A Contextual Framework for Combating Identity Theft, *IEEE Security and Privacy* (March/April), 2006, pp. 30-38.

Weick, K. E. *Sensemaking in Organizations*. Sage Publications, United States of America, 1995.

Wiley, N., The Micro-Macro Problem in Social Theory, *Sociological Theory* 6, 1988, pp. 254-261

Acknowledgements

We acknowledge and thank the Australian Transaction Reports and Analysis Centre (AUSTRAC) Steering Committee, the Australian Research Council (ARC), and industry linkage partners for monetary and in-kind contributions to this research project.

Copyright