2008

Developing a Conceptual Framework for Identity Fraud Profiling

Angela Brungs
University of New South Wales, r.jamieson@unsw.edu.au

Donald Winchester
University of New South Wales, d.winchester@unsw.edu.au

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

Stephen Smith
University of New South Wales, stephen.smith@unsw.edu.au

Recommended Citation

Brungs, Angela; Winchester, Donald; Stephens, Greg; and Smith, Stephen, "Developing a Conceptual Framework for Identity Fraud Profiling" (2008). *ECIS 2008 Proceedings*. 201.
http://aisel.aisnet.org/ecis2008/201

DEVELOPING A CONCEPTUAL FRAMEWORK FOR IDENTITY FRAUD PROFILING

Jamieson, Rodger, University of New South Wales, Sydney, NSW, 2052, Australia, r.jamieson@unsw.edu.au

Winchester, Donald, University of New South Wales, Sydney, NSW, 2052, Australia, d.winchester@unsw.edu.au

Stephens, Greg, University of New South Wales, Sydney, NSW, 2052, Australia, g.stephens@unsw.edu.au

Smith, Stephen, University of New South Wales, Sydney, NSW, 2052, Australia, stephen.smith@unsw.edu.au

Abstract

This paper addresses three main areas and develops a conceptual framework for identity fraud profiling. First, we identify the main contemporary profiling methods that are crime and/or business based. Second, accepting the current information systems (IS) facilitated attack channels and methods used by identity crime perpetrators (Jamieson & Stephens & Winchester 2007), we investigate how to best profile identity crime/fraud perpetrators. Here we are guided by relevant components of current business and crime profiling techniques. Second, analysis of interview data from industry and government agency participants was carried out using a modified grounded theoretical approach and concept mapping. Third, we consider, what identity fraud profiling systems target victim organisations might use and implement. We provide a definition for identity fraud profiling grounded from expert interviews, and based on profiling and identity crime literature. The major contributions of this paper are formation of an identity fraud profiling definition, construction of a profiling classification taxonomy, and development of an identity fraud profiling conceptual framework. This also involves providing an understanding of the framework's main elements, their relationships and application to identity fraud profiling. This framework will be useful to law enforcement, industry organisations, and government agencies when fighting to deter, detect, and prevent identity crime.

Keywords: Identity attributes, information systems (IS), identity crime, identity fraud, identity theft, identity deception, profiling, identity fraud profiling.

Acknowledgements

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

1 INTRODUCTION

The accumulated losses caused by identity crime and related crimes (money laundering, terrorism, trafficking – drugs, people, weapons, etc.) globally were estimated at up to US$2 trillion by the end of 2005 (Gordon & Willox 2006, Media-Newswire 2007). These costs are a significant motivation for identifying identity crime/fraud profiling methodologies, tools and solutions to deter, prevent and detect identity crime events. Other motivations for identity crime profiling include: "profiling is a powerful, critical and worrying technology because it is probably the only way that massive volumes of data about individual and group behaviour can be mined, whether for nefarious or benign purposes" (Hildebrandt & Backhouse 2005, p. 1); is a means to reduce organisations potential exposures through detection of identity crime acts; is an active strategy to mitigate the real threat of identity crime; profiling has deterrence and prevention effects from good intelligence to detect perpetrator identity crime innovations; and to combat identity fraud by limiting its spread or in a monitoring role (De 2004). In addition, profiling is a powerful method to summarise data/information to be better able to manage identity crime data or information from many disparate information systems (IS) or knowledge management systems (KMS) online or offline via information sharing.

Identity crime is a general term covering identity fraud, identity theft, and identity deception (Lockhart & Jamieson & Winchester & Sarre 2007, Wang & Chen & Aatabakhsh 2004). Identity fraud "refers to the gaining of money, goods, services or other benefits through the use of a false identity" obtained via preceding identity theft and/or identity deception acts (Australasian Centre for Policing Research 2006, p. 9). Identity theft is the theft of an individual's or organisation's 'identity' attribute or their personal identifying information (PII) authentication details. Identity deception (also known as assumed identity, false identity, fictitious identity, fraudulent identity, synthetic identity fraud, etc) is the obtaining of another's identity (real, lent or fictitious) attributes or authentication details by deception (Lockhart & Jamieson & Winchester & Sarre 2007). Opportunities have arisen for perpetrators of identity fraud to exploit the current situation through: the anonymity afforded in IS by Internet/mobile technologies; multi-jurisdictional issues; and privacy laws. Personal identifying information such as, PINs, passwords, key tokens, and biometrics when issued are often linked to other underlying 'identity attributes' or proof of identity (POI) data. Data in the form of POI documentation and PII are critical to identity fraud perpetrator(s) success. Proof of identity information includes: biometric (e.g., fingerprints); attributed (e.g., your full name); and biographical (e.g., education or employment history) 'identity' attributes. Contemporary profiling methods, categories of identity fraud perpetrators, perpetrator attack methods, and identity attributes in the form of POI documentation or PII will be guiding concepts for an identity fraud/crime profiling definition and conceptual framework.

"Profiling has the potential for use in identity fraud, yet its use and effectiveness for industry has not yet been studied" (Le Lievre & Jamieson 2005, p. 2). This study elaborates on the identified gap in the literature. The aim of our paper is to develop a taxonomy identifying what, where and how profiling is currently being used to help profile identity fraud perpetrators and their attacks, and to develop a conceptual framework of identity fraud profiling. Our proposed definition of profiling for identity fraud is: "the identification, collection and analysis of personal identity information, to build a profile of a perpetrator, including: biometric; attribute; and biographical attributes. These attributes identify an identity fraud perpetrator through attempting to or having gained proof of identity (POI) documentation and/or personal identifying information (PII) details from targeted entity victims (organisations, trusts, partnerships or individuals etc) through a continuum of methods defined either as identity theft or identity deception". This paper is arranged as follows: Section 2 reviews the identity crime and related profiling literature. Section 3 describes the profiling theoretical framework. Section 4 sets out our methodology. Section 5 discusses interviewee information. Section 6 briefly explains the implications and limitations of the paper. Section 7, concludes and discusses our future research program.

2 LITERATURE REVIEW

Profiling comes in many forms and interacts with IS environments (Clarke 1993) when seeking to mitigate abuse (Straub & Nance 1990) and other criminal acts offline or online (Casey 2000), including identity crimes such as identity theft, identity deception, and identity fraud (Le Lievre & Jamieson 2005). Examples of profiling in an IS context, include: behavioural profiling (Egger 1999, Turvey 2000); geographical profiling (Rossmo 2000); user profiling (Fawcett & Provost 1997); intrusion detection/network profiling (Dickerson & Dickerson 2000); customer profiling (Wiedmann & Buxel & Walsh 2002); transactions/applications profiling (Fawcett & Provost 1997, Urgaonkar & Shenoy & Roscoe 2002); identity fraud profiling (De 2004, Le Lievre & Jamieson 2005); and identity fraud related crimes, such as, terrorist profiling (Ballard & Hornik & McKenzie 2002, Davies 2003), and drug trafficking profiling (Batton & Kadleck 2004, Becton 1987). Profiling methods from both crime and business categories also have a large IS component in data and digital image storage for later retrieval and analysis through information sharing, data matching (often called computer matching in the US) and data mining techniques. Sometimes data is collected without permission or knowledge of the user e.g., CCTV, cookies, etc.

Profiling may be scientific or non-scientific (Hicks & Sales 2006), singular or aggregative (Marx & Reichman 1984), and proactive or reactive (Fredrickson & Siljander 2002). Crime profiling of the offender/perpetrator can also follow the methodology of organised (above average traits e.g., intelligent quotient (IQ), competent) or disorganised i.e., below average IQ, inadequate (Petherick 2006). Profiling techniques, aided by machine learning programs, can be classified as supervised or unsupervised. An example, of unsupervised learning includes profiling of superimposed frauds in the telecommunications and mobile phone sectors. The many types of profiling may also be categorised according to their underlying focus, for example, crime profiling, business (i.e., sometimes called marketing and/or consumer) profiling, and fraud/identity crime profiling. Moreover profiling in an IS sense "constitutes multi-factor screening (if conducted on transactions) or multi-factor file-analysis (if conducted at some subsequent time)" (Clarke 1993, p. 5). Scientific modeling should distinguish itself from non-scientific models of profiling according to the following "scientific criteria: development of a theory about profiling (e.g., criminal); hypothesis generation; operationalisation of methods used in profiling; and empirical validation, including a consideration of both disconforming evidence and the limitations of the supporting research" (Hicks & Sales 2006, p. 87).

As a scientific method, "profiling can be viewed as pattern recognition through systematically collecting, organising and analysing information collected by observation or measurement, drawing conclusions in assessing criminal suspicion, and sharing data with others where there are no privacy restrictions or other legal impediments. The method demands that procedures be objective or free from personal bias and emotion. Increased objectivity allows a knowledgeable person to check the data, as required" (Gallo 2003, p. 18). However, other views have posited that "a criminal profile is more of an educated surmise and/or a non-scientific opinion" (Turvey 2000, p. 4). When investigators use profiling to try and solve crimes that have already happened they are being reactive. Proactive profiling involves attempts to inhibit and stop crime before it happens, and has been defined, "to make judgments about another, relative to possible criminal activity, based on a number of overt and subtle factors which may or may not include things such as a person's race, manner of dress and grooming, behavioural characteristics, when and where (geographical) the observation is made, the circumstances under which the observation is made, and relative to information the officer (law enforcement) may already possess" (Fredrickson & Siljander 2002, p. 15). Singular profiling looks at discrete elements or acts, for example, a male purchasing a one-way airline ticket. Aggregative profiling involves the "reoccurrence of characteristics that eventuating once would not raise alarm. Yet with their occurrence across events should raise alerts for further inspection" (Marx & Reichman, p. 431).

At present there is very little published research on identity crime profiling techniques. An exception is a paper by ID Analytics (Fest 2005) that studied criminals who trafficked in fake (i.e., identity deception) and stolen (identity theft) identities over a two-year period. The study analysed 300 million account applications and observed several 'tactics' and 'patterns of behaviour' used by perpetrators using true-name fraud (identity theft) and synthetic identity fraud (identity deception). They found that "these guys (perpetrators) perform true-name fraud or synthetic identity fraud – but they do not do both" (Fest 2005, p. 12). The tactics adopted by "'synthetic fraud rings' (demonstrated) preference for creating female names (with) almost 63 percent of false identities (being) …woman's names, compared to just 44 percent in identity theft cases" (Fest 2005, p. 13).

In addition, two identity fraud profiling studies that help fill this void are papers that propose an outline for the role of profiling (De 2004) and an initial conceptual model (Le Lievre & Jamieson 2005) for identity fraud. De (2004) discusses the role of profiling in the detection and prevention of identity fraud within a 'crime' and under a 'systems' context. The systems perspective was considered because, the profiling techniques are most likely to be implemented in computer systems (i.e., data can be digitised, matched, shared). The research by De (2004) further discusses the 'utility' of using profiling in combating identity fraud, as well as potential limitations of its nature as not being currently in wide use and public. These limitations to its wider use include privacy or unethical issues and the property rights or sensitive nature of the operations and systems within the 'black box' that run the profiling algorithms and procedures, especially if they were to fall into the hands of the unscrupulous or even perpetrators themselves. De (2004) made several findings in his research. First, three issues were found that made it difficult to combat identity fraud including: appropriate definitions of identity fraud and related terms; commercial business constraints in the form of cost and benefits; and privacy. Second, five barriers to identity fraud profiling uptake were found, including: cost-benefit rewards; adequacy of current methods; robustness of unique personal identifiers; the structure of organisational systems; and privacy issues. Since 2004 these difficulties and barriers are now less restrictive. A study by Le Lievre and Jamieson (2005) puts forward an initial pre-conception model of identity fraud profiling. In their model they highlight five sequential stages from perpetrator, mode of attack, target system, target entity, through to the victim and suggest that "as a profile carries limited value independently it is important to analyse the interactions of profiles, which may carry more value for identity fraud detection and prevention strategies" (Le Lievre & Jamieson 2005, p. 5). Building a comprehensive understanding of the way personal documentation and information is obtained by perpetrators is one of the best mitigation strategies for identity fraud – profiling does this.

3 THEORETICAL FRAMEWORK – PROFILING TAXONOMY

Table 1 summarises various crime and business profiling methods. It outlines the profiling name, profiling domain, gives a brief description, then provides profiling basis, context with respect to ability to computerise (in terms of collating, storing, analysing, matching, or sharing the data or information), and theoretical background with example authors in that profiling domain. There are five panels in Table 1 each classifies a different profiling category. The first category is crime profiling in Panel A. Business profiling, fraud profiling and identity fraud related crimes profiling, and identity fraud profiling categories are shown in Panels B, C, D, and E respectively. As outlined in Table 1 a wealth of available literature refers to profiling in various terms, including offender profiling, criminal profiling, geographical profiling, criminal personality profiling, behavioural profiling, psychological profiling, and criminal investigative analysis (Nathan 2005). Profilers use inductive/deductive strategies, intuition or investigative psychology based on clinical, environmental, social analysis, cognitive psychology, forensic psychiatry and law enforcement principles. "Despite these conceptual differences, authors generally define profiling as interpreting crime scene behaviour in order to devise an offender profile covering gender, age, race, intelligence, interpersonal relationships, employment and location" (Nathan 2005, p. 1).

Profiling Name	**Profiling Domain**	**Description**	**Type/basis**	**Context: Ability to Computerise***	**Theory/ Background (e.g., Author/s)**
Panel A: Crime Profiling Methods					
Deoxyribonucleic acid (DNA)	Crime	An individual's unique sequence of DNA base pairs left at crime scene	Biometrics Biological	High	Genetics and biological science (Aitken 1995)
Criminal/ Offender	Crime	Behaviours, characteristics, and history of perpetrator or left at a crime scene allows inferences to be made about the offender	Behavioural, Demographical	Medium to high	Psychological/ Behavioural Science (Cook & Hinman 1999, Hicks & Sales 2006, Petherick 2006, Turvey 2000)
Organised Crime	Crime	Group of persons (>3) organise to commit a crime for profit e.g., Mafia, Bikers, Al-Qa'ida	Sociology and behavioural	Low to medium	Sociology and behavioural (Hicks & Sales 2006)
Crime Scene	Crime	Make inferences from behaviours and characteristics left at a crime scene	Behavioural/ Psychological	Medium	Forensics/Spatial/ Behavioural Science (Davis 1999)
Racial	Crime	Race, colour, ethnicity, ancestry, religion, or place of origin used to determine profile	Race and ethnicity	Medium to high	Genealogy (Batton & Kadleck 2004, Davies 2003, Hing 2006)
Psychological/ Behavioural	Crime	Applicable for serial crimes – analyse, deduce patterns	Psychology and personality	Low to medium	Psychological/ Behavioural (Egger 1999, Turvey 2000)
Demographic (also Geodemographic)	Crime/ Commerce	Demographics are used to segment/cluster individuals into groups -also using location/GPS (Global Positioning System)	Demographical	High	Media studies, advertising, marketing, and polling (Mowen & Minor 1998, Rossmo 2000)
Geographic/Investigative psychology)	Crime/ Commerce	Location and distance between locations	Spatially	High	Spatial, psychological, criminological (Canter 2003, Rossmo 2000)
Victim/target	Crime/ Commerce	Permits inferences to made about perpetrator	Behavioural/ Demographical	Medium to high	Psychological/Behavioural Science (Canter 2003, Petherick 2006, Turvey 2000)
Intelligence Quotient (IQ)	Crime/ Commerce	Intelligence	Personality	Medium to high	Intelligence (Miller 1995)
Panel B: Business/Consumer Profiling Methods					
Customer (Offline & Online Profiling)	Commerce	Analyse customers' behaviour and preferences (when online often without customers knowing or permission) for marketing/targeting to	Personality	High	Behavioural Science (Clarke 1993, Wiedmann & Buxel & Walsh 2002)
Personal Customer	Commerce	Accumulation of data concerning a particular individual - to market to	Personality and Demographical	High	Behavioural Science/ Marketing/Data Surveillance (Clarke 1993, Wiedmann & Buxel & Walsh 2002)

Abstract Customer	Commerce/ Crime	Describes a general class of person for comparison purposes against a larger data set	Personality	High	Behavioural Science/ Marketing/Statistical (Clarke 1993)
Application	Commerce/ Crime	Assemblage of metadata element selected from one or more metadata schemas and combined	Personality	High	Behavioural Science (Urgaonkar & Shenoy & Roscoe 2002)
Panel C: Fraud Profiling Methods (IS Enabled)					
Continuous Audit/Assurance	Crime/ Commerce	Evaluate system design and error-prevention procedures	Systems	High	IT/Engineering/Auditing (Loh & Jamieson 2002)
Intrusion (e.g., Anomalies)	Crime	Analyse intruders behaviour and attack modus operandi (MO)	Personality	High	Behavioural Science (Dickerson & Dickerson 2000, Wang & Guan & Zhang & Yang 2006)
User/Transactions	Crime/ Commerce	Analyse users' behaviour and preferences history for marketing/targeting or to stop transactions	Personality	High	Behavioural Science (Adomavicius & Tuzhilin 1999, Fawcett & Provost 1997)
Panel D: Identity Fraud Related Crimes Profiling Methods (i.e., Identity Theft, and/or Identity Deception Enables and Facilitates these Crimes)					
People Trafficking	Crime	Couriering of people across jurisdictions	Behavioural	Medium	Behavioural (Hing 2006)
Drug Trafficking	Crime	Importation of illegal drugs across jurisdictions	Behavioural	Medium	Behavioural (Batton & Kadleck 2004, Becton 1987)
Hijacking (Airline)	Crime	Take hostages to make demands/statement (e.g., political)	Behavioural	Medium	Psychological/ Behavioural (Hing 2006)
Money Laundering	Crime	The manipulation and use of money or property to hide its illegal source	Behavioural	High/Medium	Behavioural Science (Cuellar 2003)
Terrorist/Arms/ Trafficking	Crime	Terrorism acts and events/Importation and couriering of illegal arms or weapons across jurisdictions	Behavioural	Medium	Psychological/Behavioural (Ballard & Hornik & McKenzie 2002, Davies 2003, Hing 2006)
Panel E: Identity Fraud/Fraud Profiling Methods (also Identity theft and identity deception)					
Identity Fraud/ Theft /Deception	Crime	Biometric, biographical, and attributed identity characteristics	Potentially all of above	Medium to high	Behavioural Science (De 2004, Le Lievre & Jamieson 2005)

Table 1. Profiling Taxonomy of Crime, Business/Consumer, Fraud, Identity Fraud Related Crimes, and Identity Fraud Profiling Methods.

* The ability to computerise is in terms of collating, storing, analysing, matching, or sharing the data. High means the underlying data is mostly stored digitally; medium means usually in digital format; and low means underlying data is seldom stored digitally for analysis or sharing at sometime etc.

"Induction and deduction are among the most pivotal theoretical and practical issues in criminal profiling, yet they are the most poorly understood. Induction involves statistical or correlational reasoning whereby the current offender is assessed by virtue of their difference or similarity to past like offenders. Deduction, on the other hand, involves in-depth analysis of the current case and involves reasoning where, if the evidence collected is accurate, then the conclusions which flow from that evidence must also be accurate" (Petherick 2006, p. 1). Inductive criminal profiling develops its profile of a suspect based on the results gathered from other crime scenes. Further, inductive criminal profiles draw on formal and informal studies of known criminals, on the experience of the profiler, and on publicly available data sources, to provide guidance. The term and concept of 'profiling' has come to have many different meanings. The Federal Bureau of Intelligence (FBI) examines physical and behavioral evidence of an offense after it has occurred and, based on that information, draw inferences about potential characteristics of the person who committed the crime. On the other hand, counterterrorism is primarily concerned with the identification and interruption of terrorist activity before an attack occurs. In summary, identity fraud profiling can benefit from elements of all profiling methods outlined in our first four categories of profiling methodologies in Panels A-D of Table 1. Specific methods and their concepts will be beneficial to identity fraud profiling due to their high computerisation and implementation within a KMS context (i.e., ability to share, match or mine data) and environment included: geographic profiling; abstract profiling; application profiling; intrusion profiling; user profiling (transactions profiling); activity profiling; and money laundering profiling.

4 RESEARCH METHODOLOGY

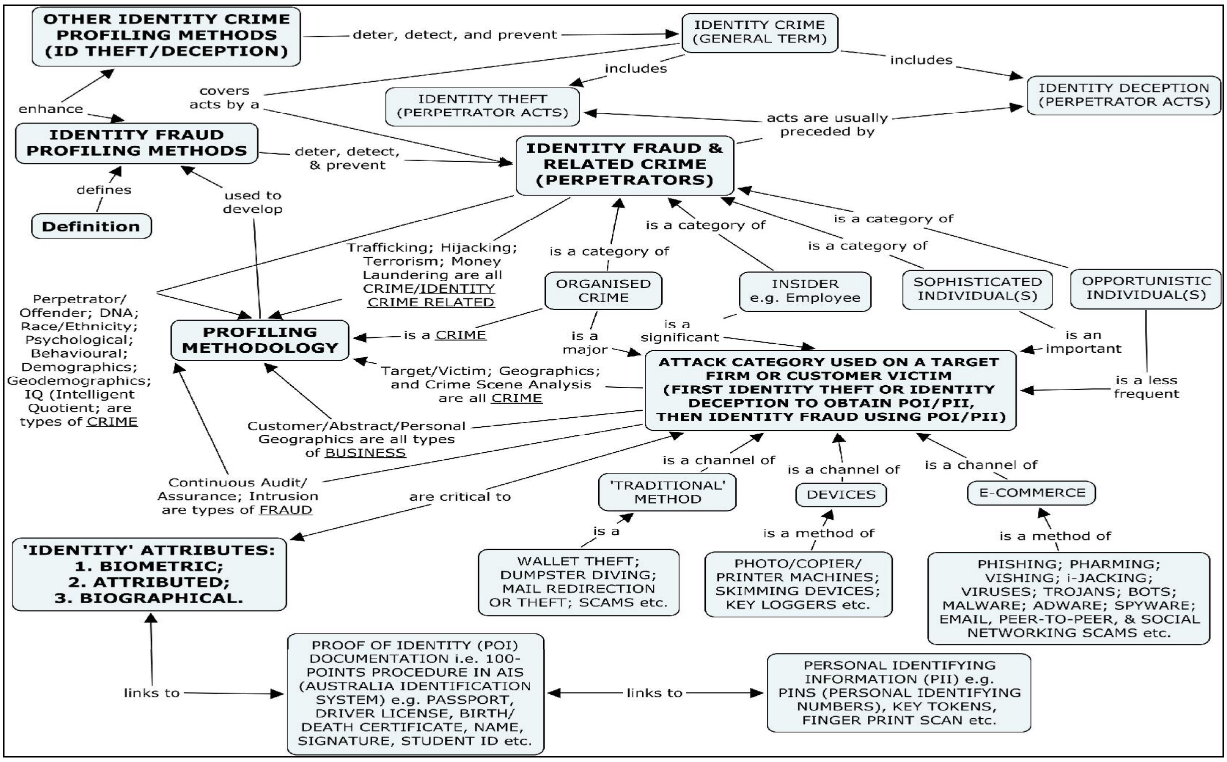
Research questions for this study of identity fraud profiling include:

- What is identity fraud profiling?
- What profiling methods are available that could be applied to identity fraud?
- What concepts surrounding these methods are best suited to an identity fraud profiling framework?

Because direct access to identity fraud perpetrators' behaviour is often restricted, we are limited in our ability to develop empirically based theories specifically on perpetrator identity fraud profiling. Therefore we must rely more on existing general profiling techniques of crime, business/consumer, fraud, identity fraud related crimes, and interviews of industry experts of targeted organisations to understand the identity crime phenomenon for identity fraud profiling. In an effort to identify what these existing theories suggest about profiling, a literature review is conducted to identify similarities and differences among profiling methodologies relevant to further developing identity fraud profiling methods. For our selected interviews, modified grounded theory was used. Grounded theory is defined as a "general methodology for developing theory that is grounded in data systematically gathered and analysed. Theory evolves during actual research, and it does this through continuous interplay between analysis and data collection" (Strauss and Corbin 1994, p. 273). Over 26 experts from 12 different organisations (banks, retailers, national and State government agencies who are issuers and users of POI) were interviewed. Interviews were recorded, transcribed, checked, and coded using qualitative software (NVivo 2, QSR International). The majority of participant interviews were face-to-face with duration of about 90 minutes. Two out of state organisation's interviews were by teleconference. Researchers have documented a need and a plan for identity crime research (Gordon & Willox 2006, Le Lievre & Jamieson 2005). We develop our profiling classification taxonomy (Table 1) and use a cognitive mapping tool (Cmap 4.12) to construct an identity fraud profiling framework (Figure 1).

5 IDENTITY FRAUD PROFILING FRAMEWORK DEVELOPMENT

Concept mapping software (Cmap 4.12) and a modified grounded theoretical approach guided the development of themes and linkages between the concepts in the identity fraud profiling model (see Figure 1). Six main themes (bolded) emerged with the support of a literature review on contemporary profiling methods, semi-structured interviews of government agency and private sector industry experts, development of our definition for identity fraud profiling, and prior identity crime/fraud research classifying identity fraud perpetrators and their attack methodologies (Jamieson & Stephens & Winchester 2007). We discuss the top level themes in Figure 1 in the following subsections, commencing with identity attributes and ending with identity fraud profiling methods.



OTHER IDENTITY CRIME PROFILING METHODS (ID THEFT/DECEPTION)
deter, detect, and prevent
IDENTITY CRIME (GENERAL TERM)
includes
includes
IDENTITY DECEPTION (PERPETRATOR ACTS)
enhance
covers acts by a
IDENTITY THEFT (PERPETRATOR ACTS)
acts are usually preceded by
IDENTITY FRAUD PROFILING METHODS
deter, detect, & prevent
IDENTITY FRAUD & RELATED CRIME (PERPETRATORS)
defines
used to develop
Definition
is a category of
is a category of
is a category of
is a category of
Trafficking; Hijacking; Terrorism; Money Laundering are all CRIME/IDENTITY CRIME RELATED
ORGANISED CRIME
INSIDER e.g. Employee
SOPHISTICATED INDIVIDUAL(S)
OPPORTUNISTIC INDIVIDUAL(S)
Perpetrator/ Offender; DNA; Race/Ethnicity; Psychological; Behavioural; Demographics; Geodemographics; IQ (Intelligent Quotient; are types of CRIME
PROFILING METHODOLOGY
is a CRIME
is a major
is a significant
is an important
is a less frequent
Target/Victim; Geographics; and Crime Scene Analysis are all CRIME
ATTACK CATEGORY USED ON A TARGET FIRM OR CUSTOMER VICTIM (FIRST IDENTITY THEFT OR IDENTITY DECEPTION TO OBTAIN POI/PII, THEN IDENTITY FRAUD USING POI/PII)
Customer/Abstract/Personal Geographics are all types of BUSINESS
Continuous Audit/ Assurance; Intrusion are types of FRAUD
are critical to
is a channel of
is a channel of
is a channel of
'TRADITIONAL' METHOD
DEVICES
E-COMMERCE
is a
is a method of
is a method of
'IDENTITY' ATTRIBUTES: 1. BIOMETRIC; 2. ATTRIBUTED; 3. BIOGRAPHICAL.
WALLET THEFT; DUMPSTER DIVING; MAIL REDIRECTION OR THEFT; SCAMS etc.
PHOTO/COPIER/ PRINTER MACHINES; SKIMMING DEVICES; KEY LOGGERS etc.
PHISHING; PHARMING; VISHING; i-JACKING; VIRUSES; TROJANS; BOTS; MALWARE; ADWARE; SPYWARE; EMAIL, PEER-TO-PEER, & SOCIAL NETWORKING SCAMS etc.
links to
PROOF OF IDENTITY (POI) DOCUMENTATION i.e. 100-POINTS PROCEDURE IN AIS (AUSTRALIA IDENTIFICATION SYSTEM) e.g. PASSPORT, DRIVER LICENSE, BIRTH/ DEATH CERTIFICATE, NAME, SIGNATURE, STUDENT ID etc.
links to
PERSONAL IDENTIFYING INFORMATION (PII) e.g. PINS (PERSONAL IDENTIFYING NUMBERS), KEY TOKENS, FINGER PRINT SCAN etc.

Figure 1. Framework for Developing an Identity Fraud Profiling Conceptual Model

5.1 ‘Identity’ Attributes

Reinforcing the reliance on identity attributes we posited in the introduction, there are three main identity attributes (biometric, attributed, and biographical) that link to proof of identity documentation in the Australian Identification System. Identity attributes linked to POI documents and personal identifying information is critical to ‘attack category used on a target firm or customer victim’. This is the underlying information a perpetrator seeks, through identity theft or identity deception, to commit identity fraud acts against targets to secure money or assets. Biometric attributes are becoming more important and constitute inclusion on an expanding number of different POI documentation e.g., passports. Due to the underlying data, being based on attributes such as finger prints, face geometry, DNA or voice patterns that do not change (substantially) over an individual’s life. Past reliance on attributed and biographical attributes is waning due to perpetrators ability to compromise this on POI documents more easily. In a growing number of cases perpetrators just invent identity detail (i.e., identity deception). Two interviewee (National Government Participant) examples that supported the identity attributes theme and concept links were:

“Talking about the hundred points system, if the documents can be false, what’s the point?’ One area of interest will be, is it a fact that the more documents you make someone produce and of more different types in a particular name, is it more likely that they’re actually real? If I’ve actually got an electricity bill with my home address, does that mean that it’s a stronger system? Passwords and PINs do they make it stronger or not, given that we all use these things to prove our identity? Or questions where they go, ‘just give us your mother’s maiden name?’, and I go ’it’s Smith’?

Our long term strategy is a whole of government approach ultimately to getting better integrity into our documents and having better means of validating documents. Also better methodologies on how perpetrators are getting hold of the documents? I mean in terms of strengthening the types of documents we have so that they can't be copied. And the biometrics side - what are the best ways of using biometrics? Is having a photo or thumb print on a document the best way to go?

5.2 Perpetrator Attack Category Used on Target Firm of Customer Victims

Recent identity crime models (Jamieson & Stephens & Winchester 2007) categorise perpetrators, identify groups of methodologies in use and illustrate underlying actual methods in these groups to gain POI or PII details. In Figure 1, perpetrators categories are illustrated as concepts 'organised crime', 'insiders', 'sophisticated ' and 'opportunistic individuals'. Perpetrator channels are shown as 'traditional methods', devices', and 'e-commerce' concepts with examples for each given (Jamieson & Stephens & Winchester 2007). It is these underlying techniques implemented by perpetrators that are the key to the perpetrator gaining identity details permitting identity fraud acts to be initiated against target organisations (Jamieson & Stephens & Winchester 2007, Lockhart & Jamieson & Winchester & Sarre 2007).

5.3 Identity Fraud and Related Crime Perpetrators

To the casual observer identity fraud may give the impression of a serious economic crime that targets organisations such as financial institutions, and that it is a victimless non-violent crime. The reality is that identity fraud can be a violent crime as it is an enabler of related crimes. A number of the related crimes are themselves enablers of or consequence of each other. Identity fraud related crime methods that are profiled include, money laundering, terrorism, hijacking (airline), drug trafficking, people trafficking, and arms and weapons trafficking. These profiling methods are established in theory and by empirical analysis on a similar basis to the crime profiling methodologies. We have categorised them separately because a major characteristic of these crimes is the underlying link to identity fraud through identity theft or identity deception, which acts as a premise for these perpetrators maintaining anonymity which, in turn, facilitates them to evade detection at least in the short to medium term.

An interviewee comment that reinforces the 'identity fraud and related crime perpetrators' theme and concept links is: "*Our analysts do work that finds information in the data and then we alert other agencies. A pattern may suggest, either drug trafficking or people smuggling or identity crime and it's amazing what sort of patterns are found. There are patterns that they can actually go – this looks like not just drug trafficking, this looks like heroin trafficking as opposed to something else. Once they've found that sort of pattern, then we are not an investigating agency at all, and it is referred off to, the police or other appropriate agencies"* (National Government Participant).

5.4 Contemporary Profiling Methods

Currently used profiling methodologies were categorised (refer Table 1) into five distinct groups – crime, business, fraud, identity fraud related, and identity fraud methods. This taxonomy allowed for deeper understanding of the distinct profiling linkages between 'attack category used on a target firm of customer victim', 'identity fraud (perpetrator)', and 'identity fraud profiling methods' themes. Interestingly a previous identified concept 'organised crime' has its own well developed profiling literature with theory and empirical studies.

Interviewee examples that help build a case for categorised contemporaneous profiling methods:
"…'look at all these hits'. All these people in the Australian Crime Commissions fraud register we've got records of transactions that they've made" (National Government Participant).
"*Recently the police came to us and said … well they think it could have been an outer state number plate at one stage and they asked us to do the scan of our database. And we gave them information*

back that met that profile. On another occasion they actually caught the offenders and charged them. We are establishing trust for assistance both ways" (State Government Participant).

5.5 Identity Fraud Profiling Methods

Interviewees monitored their businesses transactions, products, channels, employees, internal and perimeter systems and procedures in a variety of ways. These included: using third parties to acquire data to match and verify identities, off the shelf and proprietary user monitoring and authentication systems (CCTV and software), data matching, data mining, formal and informal information sharing about attacks of known perpetrators, rigorous agent (employee etc.) screening, and audits.

This paper makes the following additional contributions to identity fraud profiling methodology as a foundation for more empirical research and in developing tools and systems solutions to deter, detect and prevent identity crime/fraud. First, we provide a definition for identity fraud profiling that gives scope for developing our conceptual model, future empirics, and solutions. Second, we highlight the important links between identity attributes, POI, PII and their related critical importance to the perpetrator attack category through three previously identified channels and their underlying methods (Jamieson & Stephens & Winchester 2007). The examples of the underlying attack methods give clues of how perpetrators obtain POI/PII details and their subsequent use in identity fraud acts that need to be profiled. Third, a profiling taxonomy is used to categorise techniques where components are applicable to identity fraud profiling and we show how these links relate to the identity fraud perpetrator theme (and concept, e.g., organised crime), targeted firm and customer victims. Fourth, practitioners and our industry experts use a vast array of methods to deter, detect, and prevent perpetrators. They seek to corroborate in the background, who they are undertaking business with by validating details such as, name, address, age, mothers' maiden name, unique identifiers (alpha and numerical) on identity, passport, social security, tax, welfare, medical, licences, and student documents or cards. Most of these documents or cards are easily replicated based on real or invented individuals by perpetrators as they relied on attributed or biographical attributes and less on biometrics. Where biometrics are used, such as, signature on a cheque, photo in a passport or license, perpetrators were also able to forge or replace these biometrics by-passing those controls. Finally, to successfully profile identity fraud and related perpetrators, targeted entities need to take into account all themes and concepts shown in the cognitive framework (see Figure 1). Exact profiling is possible, but will probably need to be biometric attribute based.

6 IMPLICATIONS AND LIMITATIONS

Profiling is a broad discipline and we have categorised profiling into five main areas to facilitate our framework focusing on the identity fraud profiling research aim. This approach is to be crystallised through developing and implementing identity fraud profiling systems (techniques and tools) and strategies as part of a suite of deterrence, detection and prevention measures aimed at combating identity fraud. Moreover, appropriate legislation needs to be in place for law enforcement to be able to bring perpetrators to justice for identity crimes. Limitations to studying identity fraud profiling include IS privacy and security issues in obtaining access to perpetrators and their data for analysis purposes.

7 CONCLUSIONS

The majority of the general crime and business/customer based profiling methodologies have procedures, techniques, information collection, collation, storing, and analysis techniques applicable to developing identity fraud profiling models (systems and tools). This is especially true in an IS environment where there is the ability to computerise (digitise) data for profiling the underlying information. This is important because currently, identity fraud perpetrators are targeting financial institutions or other business sectors (e.g. government agencies, retailers, utility organisations) and online financial facilities to misappropriate funds, goods, or avoid payments or losses. Therefore the ability to mitigate these acts in real-time in an IS environment (face-to-face or customer-not-present situations) is critical. The discussion posits larger budgets for IS system upgrades, innovations and methods like, profiling as a solution to mitigate identity fraud e.g., at airports entry points. Integrating relevant techniques of the above profiling methodologies into an identity fraud profiling model should reduce the quantity of identity fraud perpetrator events and permit healthy continuation of business in legitimate organisations uninterrupted by identity crime attempts or acts.

Key barriers to the use of profiling by organisations, (especially small or micro-organisations) include, high setup and ongoing costs, the largely unquantifiable benefits of profiling identity fraud and related perpetrators, the perceived adequacy of current techniques (and their updating versions), a lack in strength of key identifying characteristics entering models (statistical errors e.g., high false positives), and the varied nature of organisational systems development (legacy issues) and ongoing legal and privacy ramifications. Biometric capture of 'identity' attributes in POI and PII should lead to exact identity profiling outcomes and reduction in identity fraud and related crimes. The contribution of this paper is our identity fraud profile definition, our classification scheme of the five profiling categories developed through our analysis of the profiling literature, and the mapping of these themes and concepts with prior identity crime models. The result is an identity fraud profiling model incorporating all these themes, concepts, and linkages. Our future research agenda includes the introduction of identity fraud and related crime profiling solutions, using methods, such as, computational immunology, for application in IS environments for use in targeted sector organisations.

References

Adomavicius, G., and Tuzhilin, A. (1999). User Profiling in Personalisation Applications Through Rule Discovery and Validation. ACM, 377-381.

Aitken, C. (1995). Statistics and Evaluation of Evidence for Forensic Scientists. John Wiley & Sons, England.

Australasian Centre for Policing Research. (2006). Standardisation of definitions of identity crime terms: A step towards consistency. Commonwealth of Australia, (March:145.3), 1-19.

Ballard, D., Hornik, J., and McKenzie, D. (2002). Technological Facilitation of Terrorism: Definitional, Legal, and Policy Issues. American Behavioural Scientist (45:6), February, 989-1016.

Batton, C., and Kadleck, C. (2004). Theoretical and Methodological Issues in Racial Profiling Research. Police Quarterly (7:1), March, 30-64.

Becton, C. (1987). The Drug Courier Profile: All Seems Infected that th' Infected Spy, as All Looks Yellow to the Jaundic'd Eye. North Carolina Law Review (65:3), March, 417-480.

Canter, D. (2003). Mapping Murder: The Secrets of Geographical Profiling. Virgin Books, London.

Casey, E. (2000). Criminal Profiling, Computers, and the Internet. Journal of Behavioural Profiling (1:2), May, 1-8.

Clarke R. (1993). Profiling: A Hidden Challenge to the Regulation of Data Surveillance. Journal of Law and Information Science (4:2), December, 1-12.

Cook, P., and Hinman, D. (1999). Criminal Profiling: Science and Art. Journal of Contemporary Criminal Justice (15:3), August, 230-241.

Cuellar, M. (2003). The Tenuous Relationship Between the Fight Against Money Laundering and the Disruption of Criminal Finance. Journal of Criminal Law & Criminology, (93:2/3), 311-465.

Davis, J. (1999). Criminal Personality Profiling and Crime Scene Assessment A Contemporary Investigative Tool to Assist Law Enforcement Public Safety. Journal of Contemporary Criminal Justice, (15:3), August, 291-301.

Davies, S. (2003). Profiling Terror. Ohio State Journal of Criminal Law, (1), 45-101.

De, K. (2004). The Role of Profiling in the Detection and Prevention of Identity Fraud. Unpublished Dissertation. University of New South Wales.

Dickerson, J., and Dickerson, J. A. (2000). Fuzzy Network Profiling for Intrusion Detection. Electrical and Computer Engineering Department Iowa State University, 1-6.

Egger, S. (1999). Psychological Profiling: Past, Present and Future. Journal of Contemporary Criminal Justice, (15:3), August, 242-261.

Fawcett, T., and Provost, F. (1997). Adaptive Fraud Detection. Data Mining and Knowledge Discovery, (1), 291–316.

Fest, G. (2005). Profiling: The DNA of Fraud Rings. Bank Technology News, (18:7), 12-13.

Fredrickson, D., and Siljander, R. (2002). Racial Profiling: Eliminating the Confusion between Racial and Criminal Profiling. Springfield, IL: Charles C. Thomas.

Gallo, F. (2003). Profiling vs. Racial Profiling Making Sense of it All. Trainer Magazine, (18.4), July/August, 18–21.

Gordon, G., and Willox, Jr., N. (2006). The Ongoing Critical Threats Created by Identity Fraud: An Action Plan. Economic Crime Institute of Utica College, March, 1-11.

Hicks, S., and Sales, B. (2006). Criminal Profiling: Developing an Effective Science and Practice. American Psychological Association, Washington, DC.

Hildebrandt, M., and Backhouse, J., (Eds.). (2005). Descriptive analysis and inventory of profiling practices. Future of Identity in the Information Society (FIDIS), June, (1.0), 1-116.

Hing, B. (2006). Misusing Immigration Policies in the Name of Homeland Security. MUSE Project, University of California, Davis, 195-224.

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

Le Lievre, E., and Jamieson, R. (2005). An Investigation of Identity Fraud in Australian Organisations. Collaborative Electronic Commerce Technology and Research (CollECTeR), 1-10.

Lockhart, S., Jamieson, R., Winchester, D., and Sarre, R. (2007). Responding to identity fraud: Issues for Australian policy-makers. Report for the Australian Research Council Grant 2005-2008, 1-28.

Loh, S., and Jamieson, R. (2002). Continuous Assurance of E-Business Transactions for Fraud Detection. CollECTeR, 1-13. http://www.collecter.org/archives/2002_December/20.pdf

Marx, G., and Reichman. N. (1984). Routinising the Discovery of Secrets: Computer as Informants. American Behavioural Scientist, (27:4), March/April, 423-452.

Media-Newswire. (2007). Queensland Outlaws Identity Fraud. Queensland Government March, 1-2.

Miller, E. (1995). Race, Socioeconomic Variables, and Intelligence. Mankind Quarterly, 35, 267-291.

Mowen, J., and Minor, M. (1998). Consumer Behavior (5th Ed), Sage Publications, California, USA.

Nathan, G. (2005). Offender Profiling: A Review of the Literature. The British Journal of Forensic Practice, August, 1-7.

Petherick, W. (2006). Serial Crime: Theoretical and Practical Issues in Behavioral Profiling, Elsevier Inc., London, Great Britain.

Rossmo, D. (2000). Geographical profiling. CRC Press, Boca Raton, FL.

Straub, D., and Nance, W. (1990). Discovering and Disciplining Computer Abuse in Organisations: A Field Study. MIS Quarterly, (14:1), March, 45-60.

Strauss, A. L., and Corbin, J. M. (1994). Grounded Theory Methodology: An Overview", in N. K. Denzin, and Lincoln, Y. S. Editors. Handbook of Qualitative Research, Sage, Thousand Oaks, California, 273–285.

Turvey, B. (2000). Criminal Profiling and the Problem of Forensic Individuation. Journal of Behavioral Profiling, May, (1:2), 1-26. (http://www.profiling.org, accessed 1 March 2007).

Urgaonkar, B., Shenoy, P., and Roscoe, T. (2002). Resource Overbooking and Application Profiling in Shared Hosting Platforms. ACM SIGOPS Operating Systems Review, (36:SI), Winter, 239-254.

Wang, G., Chen, H., and Aatabakhsh, H. (2004). Criminal Identity Deception and Deception Detection in Law Enforcement. Group Decision and Negotiation, (13), 111–127, Kluwer Academic Publishers, Netherlands.

Wang, W., Guan, X., Zhang, X., and Yang, L. (2006). Profiling Program Behavior for Anomaly Intrusion Detection Based on the Transition and Frequency Property of Computer Audit Data. Computers & Security, (25), 539-550.

Wiedmann, K-P., Buxel. H., and Walsh. G. (2002). Customer Profiling in E-Commerce: Methodological Aspects and Challenges. The Journal of Database Marketing, (9:2), 170-184.